

CLIENT-SIDE ANTI-CHEAT IN ONLINE GAMES: LEGAL IMPLICATIONS FROM A PRIVACY AND DATA PROTECTION PERSPECTIVE

WRITTEN BY: RUBEN GREIDANUS

STUDENT NUMBER: 2005412

SUPERVISORS: COLETTE CUIJPERS & KARINE E. SILVA

WORD-COUNT (EXCLUDING INDEX, FOOTNOTES, TEXTBOXES, ETC.): 17.939

**MASTER'S THESIS WRITTEN FOR THE LAW AND TECHNOLOGY PROGRAM AT TILBURG
UNIVERSITY. JUNE 23RD, 2017.**

INDEX

CHAPTER ONE – INTRODUCTION

1.1 BACKGROUND	4
1.2 OBJECTIVES AND RESEARCH QUESTION	5
1.3 METHODOLOGY	6
1.4 LIMITATIONS AND PRELIMINARY REMARKS	7
1.5 STRUCTURE	7

CHAPTER TWO – BACKGROUND INFORMATION

2.1 INTRODUCTION	8
2.2 HISTORY	8
2.3 VIRTUAL WORLDS	8
2.4 IN-GAME ECONOMIES	9
2.5 CHEATING: BOTS AND HACKS	10
2.6 A DIGITAL ARMS RACE	12
2.7 THE ROLE OF SECRECY	12
2.8 CLIENT-SERVER ARCHITECTURE	13
2.9 CHEATS FROM A TECHNICAL PERSPECTIVE	14
2.10 DETECTION METHODS	16
2.10.1 CLIENT-SIDE DETECTION METHODS	16
2.10.2 SERVER-SIDE DETECTION METHODS	22
2.11 CONCLUSION	23

CHAPTER THREE – THE LAWFULNESS OF CLIENT-SIDE ANTI-CHEAT

3.1 INTRODUCTION	24
3.2 THE IMPLICATIONS TO PRIVACY AND DATA PROTECTION	24
3.3 A CLOSER LOOK AT THE APPLICABILITY OF THE ePRIVACY DIRECTIVE	28
3.4 EXCEPTIONS TO ARTICLE 5(3)	30
3.5 CIRCUMVENTING THE CONSENT REQUIREMENT	32
3.6 INFORMED CONSENT	33
3.6.1 THE CONTENT OF THE INFORMATION	34

3.6.2 THE WAY IN WHICH THE INFORMATION IS PROVIDED	36
3.7 INFORMED CONSENT IN PRACTICE	37
3.7.1 FINDINGS (CONTENT)	38
3.7.2 FINDINGS (CONVEYANCE)	38
3.7.3 AN EXAMPLE OF QUESTIONABLE TERMS	39
3.8 CONCLUSION	40
CHAPTER FOUR – THE RIGHT OF ACCESS TO PERSONAL DATA	
4.1 INTRODUCTION	41
4.2 QUALIFYING THE CHEATING-DOSSIER AS PERSONAL DATA	41
4.3 LIMITS TO THE RIGHT OF ACCESS	43
4.4 CONCLUSION	47
CHAPTER FIVE – RE-CONCEPTUALIZING INFORMED CONSENT	
5.1 INTRODUCTION	48
5.2 THE RIGHT OF ACCESS VERSUS THE RIGHT TO TRADE SECRETS	48
5.3 SUBSTANTIATING INFORMED CONSENT FOR THE CASE OF ONLINE GAMING	49
5.4 MAKING THE CASE FOR INFORMED CONSENT	49
5.5 INFORMED CONSENT BY WAY OF THIRD PARTY	52
5.6 CONCLUSION	59
CHAPTER SIX – CONCLUSION	
6.1 ANSWERING THE RESEARCH QUESTION	60
6.2 LIMITATIONS AND RECOMMENDATIONS FOR FURTHER RESEARCH	63
6.3 CLOSING STATEMENT	64
BIBLIOGRAPHY	66
ANNEX A	70
ANNEX B	77
ANNEX C	86

CHAPTER ONE - INTRODUCTION

1.1 Background

In 2004, twenty-four year old furniture salesman Noah Burn made tens of thousands of dollars in a matter of weeks.¹ Ask him how, and he will tell you he made the money selling furniture – but not the type you would expect. Noah was an avid player of the online multiplayer role playing game, EverQuest II. In the game, he is ‘Methical’, the gnome barbarian, and runs his own virtual store where he – somewhat ironically – sells virtual furniture. As ridiculous as this may sound, Burn found a way to break the game’s rules and was able to duplicate any piece of furniture he desired. With the help of a friend, Burn devised a way to produce and sell the furniture en masse, focusing on the most expensive pieces with the highest demand. As he explains, ‘*selling real furniture pays well, but not as well as in EverQuest II*’.² His next step was converting those virtual riches into real money. With plenty of auction sites available, Burn and his accomplice made around \$100,000 before visiting a lawyer as to inquire to the legal risks. The lawyer reportedly threw his hands up in confusion, stating that he had no idea what Burn was talking about. Sony Entertainment, the developers of the game, did eventually catch on and started wondering where all this furniture flooding the market could have possibly come from. Once Sony figured it out Burn was banned from the game. But it was too late: Sony Entertainment saw the in-game economy – a vital aspect of their online multiplayer game – take a huge hit. The damage was done and it proved to be irreversible.³

Anti-cheat, the endeavor to catch players that are using cheats or are otherwise exploiting the rules of the game⁴, is a key part of online gaming. While some game companies only perform behavioral analysis of players, some actively scan and investigate their users’ computers in order to detect cheaters. Many have expressed privacy concerns.⁵ Although the field of online gaming has received more attention from legal scholars in recent years, this particular topic has remained unexplored in academia.

¹ Tim Guest, *Second Lives* (Hutchinson Random House 2007) ch 7

² *Ibid*

³ *Ibid*

⁴ This is my own characterization as there is no definition in the literature.

⁵ See: paragraph 4.3. See also, for example: www.reddit.com/r/GlobalOffensive/comments/36o0c9/boycott_esea/;
<https://eu.battle.net/forums/en/wow/topic/9052336080>;
www.unknowncheats.me/forum/battlefield-4-a/136167-punkbuster-screenshot-confusion.html#post1144550

1.2 Objectives and research questions

Similar to spyware, ‘client-side’⁶ anti-cheat accesses and collects information from users’ computers in a way which raises legal concerns from a privacy and data protection perspective. This thesis determines if and to what extent these concerns are well-founded: (under which circumstances) is client-side anti-cheat unlawful?⁷ However, this question must also be placed in the appropriate context. There is a conflict going on between cheaters and game companies wherein both parties are trying to obscure their methods as much as possible. As I will demonstrate in chapter three and four, this interest in secrecy ultimately comes at the expense of users’ interests in transparency. In order to determine whether game companies’ interests in secrecy are legally justifiable, a brief excursion into trade-secret law is appropriate. Taking all the above into account, the main objectives of this thesis are:

1. To explore and expose the available methods of cheat detection in such a way as to make them suited for subsequent legal analysis.
2. To determine to what extent the privacy and data protection framework restricts or otherwise limits the usage of client-side anti-cheat, taking into account both direct limitations (whether the activity is lawful as such) and indirect limitations (mainly the right to access personal data).
3. To determine to what extent trade secret law mitigates the restrictions and limitations above.

The legal instruments necessary for this analysis are the Privacy and Electronic Communications Directive, the General Data Protection Regulation (henceforth: GDPR) and the Trade Secret Directive.⁸ Accordingly, this thesis will answer the following research question:

How do the ePrivacy Directive and GDPR restrict or otherwise limit usage of client-side anti-cheat by online gaming companies?

Consequently, this means answering the following sub-questions:

1. *What are cheats and how do they work?*

⁶ Client-side refers to anti-cheat that accesses information from the user’s computer.

⁷ The research question posed by this thesis (see below) is broader as it also includes indirect restrictions on game companies’ usage of client-side anti-cheat (see chapter four).

⁸ The choice for legal instruments will be further explained in chapter three.

2. *Which technological countermeasures are currently being used in detecting cheats?*
3. *How does the European Union legal framework concerning privacy and data protection restrict or otherwise limit the measures discussed in sub-question two?*

1.3 Methodology

Doctrinal legal research was chosen as the primary method because any legitimate answer to this research question can only result from a systematic analysis of legislation, case law and literature. Doctrinal research is particularly well suited to this.⁹ As was already implied, academic literature directly dealing with this particular topic is almost entirely absent; and in this regard, this thesis plays a pioneering role. Fortunately, much of the focus will be on interpreting and applying existing legal concepts to the context of client-side anti-cheat, and plenty of literature on these topics individually is available. Furthermore, because client-side anti-cheat exhibits similarities to spyware, legal sources dealing with that subject can also be drawn from. Because technological literature dealing with client-side anti-cheat is also scarce, semi-structured interviews will be used as a supplementary source of information.¹⁰¹¹¹² Lastly, several terms of service and privacy policies have been reviewed in order to better substantiate the theoretical analysis in chapter three.¹³ Third party anti-cheat software was selected randomly, although ESEA was explicitly included due to the fact that its policy appeared salient for further analysis.¹⁴

⁹ Terry Hutchinson, 'The Doctrinal Method: Incorporating Interdisciplinary Methods in Reforming the Law' (2015) 3 *Erasmus Law Review* 130

¹⁰ To be clear, these interviews are intended to be a supplementary source of information rather than a basis from which to draw empirically sound conclusions. As such, the interviews were conducted in an informal, loosely structured manner and no in-depth attention will be paid here to methodology (as would have been the case if the interviews were intended for qualitative research purposes).

¹¹ Two respondents participated. One has a great deal of experience with reverse engineering cheat and bot-detection mechanisms while the second participant has significant technical knowledge concerning bots, cheats and the ways in which they interact with games. Both participants had their names anonymized.

¹² Note: the transcripts have been slightly modified for readability.

¹³ Because no decisive ranking regarding popularity exists, noteworthy (i.e. games with high player-counts or recent releases) games were randomly selected from several listings/rankings.

¹⁴ Once again, the objective of this review is not to provide an empirically sound, quantitative analysis of such terms. Rather, the focus is on providing illustrative examples which help further concretize the theoretical discussion by way of example.

1.4 Limitations and preliminary remarks

It should be noted that, due to interests in secrecy on the part of game companies, some parts of this thesis have been based partly on speculation. For example, chapter four presupposes that companies keep records on cheaters, but arrives at this conclusion not by empirical verification but rather by way of logical reasoning. It should also be emphasized that this thesis is limited in the sense that it is the only comprehensive piece of legal work currently available on the matter. As a result, many original assertions have been made without the luxury of an already existing body of legal knowledge and debate to fall back on.¹⁵

1.5 Structure

Chapter two is descriptive in nature and provides both the background information and technical explanations necessary for the subsequent legal analysis. Building on this, chapter three examines the lawfulness of client-side anti-cheat. Chapter four examines the way in which the right of access to personal data indirectly further restricts game companies in their usage of anti-cheat. Chapter five explores and discusses the tension between informed consent and game companies' interests in secrecy and how this tension should be resolved. Lastly, the conclusion summarizes and consolidates the main findings.¹⁶

¹⁵ This pioneering role is on the one hand its greatest strength but on the other also its greatest weakness. While I am very confident in the quality of my work, none of it should be taken as gospel and I therefore encourage other authors to be critical and to introduce their own ideas and interpretations into the debate.

¹⁶ To summarize, chapter two answers sub-questions 1 and 2, while chapter three, four and five answer sub-question 3.

CHAPTER TWO – BACKGROUND INFORMATION

2.1 Introduction

This chapter explores several key concepts, necessary background information and technical explanations of the problem at hand. The first half discusses the history of (online) gaming, the concept of virtual worlds and economies, cheating in general and the context in which it takes place – essentially covering the *what*, *who* and *why*. The second part of this chapter explains *how* cheaters cheat and game companies detect from a technical standpoint.

2.2 History

Over the past sixty years, videogames have grown from a niche product into the multi-billion dollar industry it is today.¹⁷ The popularization of the internet allowed developers to expand upon on the multi-player aspect of videogames in both scale and complexity.¹⁸ In particular, massive multiplayer online games, which gained mainstream recognition with the 2004 release of the incredibly popular ‘World of Warcraft’, took the concept of multiplayer to new heights by immersing players into virtual worlds in which thousands of people play simultaneously.¹⁹

2.3 Virtual worlds

In both mainstream and academic discourse, terms such as ‘virtual worlds’ and ‘virtual economies’ are frequently used with regards to (massive) multiplayer online games, suggesting a clear separation between the real world and the game-world. This approach has garnered criticism due to the fact that such a strictly dualistic perspective may give rise to the idea that users are immune to privacy risks.²⁰ Significant scholarly debate exists with regards to this matter.²¹ Lastowska, an author who has studied online games from a legal perspective, generally

¹⁷ Jeff Desjardins, ‘The History and Evolution of the Video Games Market’ (Visual Capitalist, January 11 2016) <www.visualcapitalist.com/history-video-games-market/> accessed February 3 2017

¹⁸ Riad Chikhani, ‘The History Of Gaming: An Evolving Community’ (Tech Crunch, October 31 2015) <<https://techcrunch.com/2015/10/31/the-history-of-gaming-an-evolving-community/>> accessed February 10 2017

¹⁹ Lauren Indvik, ‘The Fascinating History of Online Role Playing Games’ (Mashable, November 14 2012) <<http://mashable.com/2012/11/14/mmorpgs-history/#s.WRo96LVsqV>> accessed February 9 2017

²⁰ Barosso and others, ‘Virtual Worlds, Real Money: Security and Privacy in Massively Multiplayer Online Games and Social and Corporate Virtual Worlds’ (2008) ENISA Position Paper

²¹ See, for example: Vili Lehdonvirta, ‘Virtual Worlds Don't Exist: Questioning the Dichotomous Approach in MMO Studies’ (2010) 10(1) Game Studies 1

argues in favor of a clear separation and states that play fails to ‘*conform to the reason and logic of ordinary life*’ and that ‘*law must consequently treat game activities differently*’.^{22,23} Others have rejected this notion and warn that the conceptualization of a clearly separated real and virtual world, although convenient and effective at eliciting lively imagery on the part of the reader, ultimately fails to recognize that the two are intertwined to a point where separation becomes almost impossible to accept.²⁴ Indeed, the argument that the reason and logic of ordinary life do not apply to games is, while not false, one dimensional. In many ways, it is true that play does not conform to such logic – and it is logical to assume that the law must treat such activities differently where necessary. What authors such as Lastowska fail to recognize is that many different types of play may exist within a game, some of which conform completely to the reason and logic of ordinary life – and can actually only be understood in that manner. As will become clear, the subject of this thesis is a prime example of that: cheats act as an external force and result in a deviation from the normal type of play as intended by the developer. Conceptualizing the problem and finding ways to address it therefore cannot be based on the ‘*dichotomous real-virtual perspective*’²⁵. Doing so would likely result in solutions which are ineffective because such a perspective does not do justice to the various privacy implications at stake.²⁶ Where anti-cheat is concerned, the privacy implications stretch far beyond that of the realm of the game itself and it is imperative to keep that in mind when analyzing the problem and ultimately working towards a solution.

2.4 In-game economies

In almost all massive multiplayer online games – and even some non-massive multiplayer games – players find or create virtual goods and may buy these from or sell these to other players. The economies created through this process have been the subject of frequent academic analysis.²⁷

²² Greg Lastowska, ‘Rules of Play’ (2009) 4(4) *Games and Culture* 379, 393

²³ Vili Lehdonvirta, ‘Virtual Worlds Don't Exist: Questioning the Dichotomous Approach in MMO Studies’ (2010) 10(1) *Game Studies* 1

²⁴ *Ibid*

²⁵ *Ibid*

²⁶ In essence, the ‘*dichotomous real-virtual perspective*’ is unable to recognize the existence of a problem because it implicitly presupposes that harms originate from and are contained to the game world.

²⁷ See, for example: Edward Castronova, ‘On Virtual Economies’ (2002) 752 CESifo Working Paper; Vili Lehdonvirta, ‘Virtual Economics: Applying Economics to the Study of Game Worlds’ (Conference on Future Play, East Lansing, 2005)

Many authors have applied traditional economic concepts such as ‘*production, labour supply, income, inflation, foreign trade and currency exchange*’ – once again demonstrating that the ‘*dichotomous real-virtual perspective*’ is difficult to uphold.²⁸ ‘Real money trading’, a phenomenon where players exchange virtual goods for real money or vice versa, is considered a problem by many players and gaming companies.²⁹ Among other things, this allows the more affluent players to purchase advantages in the game-world rather than earning it through gameplay. It is interesting to note how ‘real-world’ issues, such as income inequality, thus permeate the game world. Despite game companies explicitly forbidding it through terms and conditions and taking active steps to further discourage it, it remains a (relatively) lucrative field, at least for sellers in poorer countries.³⁰ The real-money trade market is estimated to be worth in excess of 1 billion, with roughly eighty percent of all ‘gold farmers’³¹ hailing from China.³²

2.5 Cheating: bots and hacks

Cheating is done in a variety of ways. Randell & Yan identified as much as eleven common forms of cheating in online games.³³ This thesis focuses on the two forms most likely to illicit detection methods that impact privacy or data protection rights: cheating through game client modification and scripts aimed at automation.

By hacking the game, cheaters can ignore or bend certain parts of the game’s architecture, providing themselves with advantages over others.³⁴ For example, a cheater may be able to hack a game in such a way that he is able to see through walls.³⁵ Cheating may also involve running scripts in order to execute pre-programmed actions aimed at achieving automation³⁶ Bots,

²⁸ Vili Lehdonvirta, ‘Virtual Economics: Applying Economics to the Study of Game Worlds’ (Conference on Future Play, East Lansing, 2005)

²⁹ Atsushi Fujita, Hiroshi Itsuki and Hitoshi Matsubara, ‘Detecting Real Money Traders in MMORPG by Using Trading Network’ (Seventh Artificial Intelligence and Interactive Digital Entertainment Conference, Palo Alto, 2011) 1

³⁰ Richard Heeks, ‘*Understanding ‘Gold Farming’ and Real-Money Trading as the Intersection of Real and Virtual Economies*’ (2010) 2(4) *Journal of Virtual Worlds Research* 3, 6-7

³¹ People who play games purely with the intent to collect and sell virtual goods as a source of income.

³² Richard Heeks, ‘*Understanding ‘Gold Farming’ and Real-Money Trading as the Intersection of Real and Virtual Economies*’ (2010) 2(4) *Journal of Virtual Worlds Research* 3, 7

³³ Brian Randell and Jeff Yan, ‘A systematic classification of cheating in online games’ (NetGames '05 Proceedings of 4th ACM SIGCOMM workshop on Network and system support for games, Hawthorne, 2005) 2-4

³⁴ *Ibid*

³⁵ Nick Cano, *Game Hacking: Developing Autonomous Bots for Online Games* (No Starch Press 2016) 213

³⁶ *Ibid*, 19-21

finally, can best be understood as a combination of the above. Some authors describe bots simply as ‘*auto playing game-clients*’³⁸ or ‘*stand-alone programs that play a game for you*’.³⁹ For the purposes of this thesis, I put forward a more detailed characterization in that they are best understood as an elaborate collection of scripts designed to perform automated tasks. In order to adequately and efficiently perform these tasks, they tend to interface directly with the underlying game code in order to quickly obtain information and send inputs back to the game. In some cases, they also ignore or bend certain parts of the game’s architecture to better perform these tasks. To summarize, botting is a form of cheating that uses hacks, but not every bot is a hack - hacks can also be used separately by people actively playing the game.

The most glaring concern with cheating is that is against the spirit of the game because it puts other players at a disadvantage. There is little enjoyment in playing a board game against someone who somehow rolls a six every single time. In addition, at least where massive multiplayer online games are concerned, players are rewarded for completing tasks with (among other things) virtual goods. As discussed in the previous paragraph, these virtual goods can be converted into cash through real money trading. Depending on the game and the nature and quality of a cheat, the collection process of virtual goods is automatable (with bots) or at least made easier (through hacks).⁴⁰ Other players are negatively affected by this as cheaters increase the supply of virtual goods and thus deflate the value, which is detrimental to legitimate players seeking to sell the same commodity.⁴¹ Indeed, a quick look at several online game forums reveals that many players demand that developers act strongly against cheaters.⁴² Consequently, failing to meet customer demands may lead to substantial loss of profit on the side of the gaming

³⁷ Scripts are best understood as a list of commands executed in succession.

³⁸ Chen and others, ‘Identifying MMORPG bots: a traffic analysis approach’ [2009] EURASIP Journal on Advances in Signal Processing - Special issue on signal processing applications in network intrusion detection systems 1, 1

³⁹ Chris Hogg and Gary McGraw, *Exploring Online Games: Cheating Massively Distributed Systems* (Kindle Edition, Second Printing, Pearson Education 2008) Location 999

⁴⁰ *Ibid*

⁴¹ Barosso and others, ‘Virtual Worlds, Real Money: Security and Privacy in Massively Multiplayer Online Games and Social and Corporate Virtual Worlds’ (2008) ENISA Position Paper 9

⁴² See, for example: <http://bgr.com/2016/08/19/pokemon-go-cheats-ban-tips-tricks-niantic/>;
us.battle.net/forums/en/d3/topic/19288210069;
us.battle.net/forums/en/d3/topic/19288660168;
www.pathofexile.com/forum/view-thread/911821/page/1;
<https://eu.battle.net/forums/en/overwatch/topic/17614713755>;

company, as many (massively) multiplayer online games rely on recurring purchases as their profit model.⁴³

2.6 A digital arms race

Cano describes the late 1990s to early 2000s as the ‘*golden age of game hacking, when online PC games became advanced enough to draw large crowds but were still simple enough to easily reverse engineer*’.⁴⁴ Cheating eventually became a big enough nuisance for game companies to commit more time and energy into actively developing ways to deter and detect.⁴⁵ As game companies develop more and more advanced methods of detection, however, cheaters reactively develop new ways to circumvent those methods. Some authors refer to the conflict between cheaters and game developers in militarized terms: wars, battles, arms races, and so forth.⁴⁶ The term ‘arms race’ is most suited as it captures the reactionary aspect quite well: cheaters and gaming companies are constantly trying to develop and deploy new techniques in an effort to gain the upper hand over the other party.⁴⁷

2.7 The role of secrecy

It is important to recognize the key role of secrecy. As will become clear in the following paragraphs, knowing what the other party is doing technically is essential from both a detection and circumvention standpoint. Disclosure from both parties regarding their modus operandi is therefore extremely rare. The value of such information and consequently the lengths to which game companies are willing to go in order to secure it is best made clear through an actual example. Blizzard Entertainment, one of the most well-known online gaming companies, threatened a freelance programmer at Bossland (a bot developer) by the name of Enright with legal action unless he handed over the source code of Stormbuddy, a bot made and distributed by Bossland. Enright, fearing the possible consequences of legal proceedings enacted against him,

⁴³ Justin Olivetti, ‘Massively OP’s Guide to MMO Business Models’ (*Massively Overpowered*, April 30 2016) <<http://massivelyop.com/2016/04/30/massively-ops-guide-to-mmo-business-models/>> accessed February 11 2017

⁴⁴ Nick Cano, *Game Hacking: Developing Autonomous Bots for Online Games* (No Starch Press 2016) 19-20

⁴⁵ *Ibid*, 19-20

⁴⁶ See, for example: Chris Hogg and Gary McGraw, *Exploring Online Games: Cheating Massively Distributed Systems* (Kindle Edition, Second Printing, Pearson Education 2008) Location 1805

⁴⁷ To illustrate using real-world terms, when one of two nations at war develops new missile capabilities, the other nation’s response may be a new missile defense shield, which may trigger the development of a new type of missile capable of penetrating such a shield, and so forth.

complied and handed over the source code in its entirety.⁴⁸ Letschew, owner of Bossland, claims that ‘Activision Blizzard is fully aware that Bossland GmbH, and not [Enright], is the owner of the intellectual property of Honorbuddy, Demonbuddy and Stormbuddy, considering that there are six cases that are still in progress [...] in Germany’. With the source code in Blizzard’s hands, Letschew goes on to state that ‘(...) we are sure that Stormbuddy can no longer be developed as it is, and that it can no longer be sold’.⁴⁹ Indeed, a look at the Stormbuddy forums reveals that the bot has been discontinued, demonstrating the high value of such information and maintaining secrecy.

2.8 Client-server architecture

Many modern online multiplayer games rely on a client-server architecture.⁵⁰ This means that the players (the clients) connect to the server (usually hosted by the game company). Both exchange information with one another. In-game actions performed by the client are sent to the server.⁵¹ For example, a player moves his or her character, the server notes that this character has moved position, and consequently transmits the new position to other players in the area.⁵² The advantage of client-service architecture from an anti-cheating perspective lies in the fact that the server controls the game world rather than the client. In a single-player game, it is relatively easy to hack the game and alter the game world because the process entirely takes place on the users’ computer. With a client-server architecture, however, the server controls crucial aspects of the game world.⁵³ For example, it keeps track of the amount of money that a player has accumulated and even if a cheater alters the client to send a different value with regards to the money in his

⁴⁸ Shakir Hussaini, ‘World of Warcraft Makers Continue Fight Against Bots’ (American University Intellectual Property Brief, January 28 2009) <www.ipbrief.net/2016/01/28/world-of-warcraft-makers-continue-fight-against-bots/> accessed on February 10 2017

⁴⁹ Ernesto Van der Sar, ‘Blizzard ‘Stole’ Our Source Code, Bot Maker Says’ (Torrentfreak, November 19 2015) <<https://torrentfreak.com/blizzard-stole-our-source-code-bot-maker-says-151119/>> accessed on February 10 2017

⁵⁰ Chris Hogg and Gary McGraw, *Exploring Online Games: Cheating Massively Distributed Systems* (Kindle Edition, Second Printing, Pearson Education 2008) Location 476

⁵¹ *Ibid*

⁵² Caltagirone and others, ‘Architecture for a Massively Multiplayer Online Role Playing Game Engine’ (2002) 18(2) *Journal of Computing Sciences in Colleges* 105, 108-110

⁵³ Kabus and others, ‘Addressing cheating in distributed MMOGs’ (2005) (NetGames '05 Proceedings of 4th ACM SIGCOMM workshop on Network and system support for games, Hawthorne 2005) 1-2

*‘RAM (pronounced ramm) is an acronym for random access memory, a type of computer memory that can be accessed randomly; that is, any byte of memory can be accessed without touching the preceding bytes. RAM is the most common type of memory found in computers and other devices, such as printers.’
(webopedia.com)*

possession, the server will recognize that this number is false. Thus, hacking the game becomes much more difficult: cheating, at least in its most blatant form, is made impossible.⁵⁴

2.9 Cheats from a technical perspective

Logically speaking, any cheat that bends or alters the game architecture or achieves effective automation must somehow extract information from the game. Additionally, depending on the particular cheat, it must also be able to send new or alter already existing information inside the game process. This paragraph

discusses the methods most commonly used in practice: memory reading, memory manipulation, code injection and function hooking.⁵⁵⁵⁶

Extracting information can be achieved through reading the game’s memory space in the computer’s RAM (random access memory).⁵⁷ The game world’s visual representation on the screen can ultimately be broken down into numerical values: the server assigns the player a certain location (expressed in x, y and z coordinates), a certain amount of virtual currency, and so forth.⁵⁸ By figuring out where exactly these values are stored, it is possible for cheaters to directly retrieve the information and use it to interpret the game world, even beyond what would normally be possible for a legitimate player.⁵⁹ While memory locations in games are almost always dynamic rather than static (meaning that specific data will appear in different places once

⁵⁴ *Ibid*

⁵⁵ See: Nick Cano, *Game Hacking: Developing Autonomous Bots for Online Games* (No Starch Press 2016) 25-27 and 155-157; David Krutsko, ‘Navigator – A scriptable software system for automating World of Warcraft’ (Bachelor thesis, Carleton University 2013) ch 4

⁵⁶ Many other methods exist, but discussing them all would be beyond the scope of this thesis. The choice for these methods was based on popularity and relevancy with regards to detection methods. Pixel detection, for example, is a method that reads the screen and searches for certain colors. However, it suffers from inherent limitations and is difficult to detect, and is therefore less relevant than the other methods discussed here. See also: Interview with participant #2 (Skype, February 12 2017) 90

⁵⁷ Mitterhofer and others, ‘Server-Side Bot Detection In Massively Multiplayer Online Games’ (2009) 7(3) IEEE Security & Privacy 1, 3-4

⁵⁸ Nick Cano, *Game Hacking: Developing Autonomous Bots for Online Games* (No Starch Press 2016) 89

⁵⁹ *Ibid*, 18

the process has been restarted), it is possible to anticipate where the needed values will appear through reverse engineering.⁶⁰ The process must be repeated every time game developers roll out a significant update and because updates are frequent in online games, maintaining cheat functionality can be quite time-consuming.⁶¹

In the same vein, memory manipulation is also possible.⁶² A cheater could edit the value that signals how many gold he has in his possession. However, due to the client-server architecture, such an endeavor would most often be futile. The server keeps track of the amount of virtual currency in the player's possession: the numerical representation on the client-side is merely that, a representation. The value will quickly be overwritten and once again display the actual value. Nevertheless, memory manipulation can also be used more indirectly, for example to facilitate code injection.⁶³ The latter is arguably the most powerful way for cheaters to extract and input information into the game. It essentially allows cheaters to 'inject' their own lines of code directly into the game process.⁶⁴ Once the code is present, all that remains is executing it. The most common way of doing so involves '*intercepting precise branches of execution and redirecting them to the injected code*', known as function hooking.⁶⁵ Code injection and function hooking allow cheaters to alter the game process in profound ways.⁶⁶⁶⁷ For example, where bots are concerned, rather than having to send simulated inputs in order to start a certain character action, it can directly call the appropriate function and circumvent input simulation (which has several advantages, including being more efficient). Code injection can also be used to isolate certain variables that would otherwise not be visible through memory reading.⁶⁸ Active players

⁶⁰ *Ibid*, 16

⁶¹ *Ibid*, 125

⁶² Wu-chang Feng, Ed Kaiser and Travis Schuessler, 'Stealth Measurements for Cheat Detection in Online-Games' (NetGames '05 Proceedings of 4th ACM SIGCOMM workshop on Network and system support for games, Hawthorne, 2005) 2

⁶³ *Ibid*

⁶⁴ *Ibid*

⁶⁵ Nick Cano, *Game Hacking: Developing Autonomous Bots for Online Games* (No Starch Press 2016) 176

⁶⁶ *Ibid*, 176-208

⁶⁷ See: Thomas Curda, 'Analysis and detection of online game cheating software' (Bachelor thesis, Masaryk University 2004) ch 3

⁶⁸ David Krutsko, 'Navigator – A scriptable software system for automating World of Warcraft' (Bachelor thesis, Carleton University 2013) para 4.1.2

could benefit from code injection and function hooking by granting themselves the ability to see through walls or achieve perfect aim.⁶⁹

2.10 Detection methods

In line with the client-server architecture on which massive multiplayer online games rely, detection methods either take place on the client or server level. Client-side detection seeks to identify bots by investigating information present on the player's computer.⁷⁰ Server-side detection, on the other hand, relies on (behavioral) data which is generated by the player and consequently logged by the server.

2.10.1 Client-side detection methods

A wide variety of client-side detection methods exist. Providing an exhaustive overview of these methods is not only beyond the scope of this thesis but would prove to be an impossible undertaking. Strong interests in secrecy ensure that many methods are not yet or will never become public. Moreover, detection techniques are constantly evolving. Online gaming companies devise new methods to detect cheaters while old methods become redundant. Gabe Newell, CEO of gaming company Valve, has stated that '*new cheats are created all the time, detected, banned, and tweaked. This specific VAC test for this specific round of cheats was effective for 13 days, which is fairly typical. It is now no longer active as the cheat providers have worked around it (...)*', illustrating not only that some detection methods have a lifespan, but also that this lifespan can be extremely short.⁷¹ Therefore, rather than attempting to provide an exhaustive overview of the detection methods currently in existence, this paragraph will focus more on general underlying principles behind those methods and offer a rough characterization.⁷²

One of the least technologically complex but potentially most invasive methods of detection relies on taking **screenshots** (essentially a digital photograph of whatever a monitor is displaying) on the player's computer and then transferring those screenshots for someone to

⁶⁹ See: Nick Cano, *Game Hacking: Developing Autonomous Bots for Online Games* (No Starch Press 2016) 213

⁷⁰ The client-side detection methods are discussed only from the perspective of the Windows operating system, as this is the operating system most commonly in use. Other operating systems are beyond the scope of this thesis.

⁷¹ Quoted from: www.reddit.com/r/gaming/comments/1y70ej/valve_vac_and_trust

⁷² As a final caveat, it should be noted that anti-cheat may be both incorporated into the game itself but may also be a separate, third party software application. While this makes for some technical differences, the underlying principles and legal repercussions remain the same, which is why they be addressed in conjunction.

review.⁷³ While it is unclear under which conditions such screenshots are taken, various anti-cheat software privacy policies confirm that the technique is indeed in use – although to what extent also remains unknown.⁷⁴ The underlying idea is that forbidden software will make use of graphical user interfaces or exhibit other visual signs which, if caught in a screenshot, would prove that that particular user was indeed cheating. Theoretically, if the anti-cheat software takes screenshots of the actual display (rather than just the assets rendered by the game) and the game window is out of focus, such screenshots may reveal a great deal of information about that user: private conversations, websites that are currently being viewed, credit card data and so forth.⁷⁵ Punkbuster, an anti-cheat software application that explicitly names the detection method in its End User License Agreement, goes so far as to state that any screenshot may be used for ‘*possible publication*’.⁷⁶ Other methods of detection are less blunt and take a more targeted approach. Signatures are byte patterns that are unique to specific software. With **signature based detection**, anti-cheat software seeks out specific patterns by scanning the player’s RAM and comparing the results with a signature black-list of forbidden software.⁷⁷ In a similar manner, **binary validation** targets specific areas of the player’s RAM and compares these areas to an original, ‘clean’ version of that area.⁷⁸ If the contents of the memory space deviate from the expected content composition, a signal is sent back to the game developer.⁷⁹ Binary validation is

⁷³ Nick Cano, *Game Hacking: Developing Autonomous Bots for Online Games* (No Starch Press 2016) 269

⁷⁴ See: https://play.esea.net/?s=content&d=privacy_policy

⁷⁵ To be clear, it is unknown whether these screenshots only target assets rendered by the game or the entire display. See: Interview with participant #2 (Skype, February 12 2017) 87

⁷⁶ See:

http://manual.americasarmy.com/index.php/I_agreed_to_the_Punkbuster_EULA_when_I_installed_America's_Army_but_didn't_read_it._Can_I_read_it_now%3F

⁷⁷ Nick Cano, *Game Hacking: Developing Autonomous Bots for Online Games* (No Starch Press 2016) 269-270

⁷⁸ The techniques here could theoretically also target the hard-disk. The principle is the same however, and because scanning hard-disks seems to be rarely done or mentioned, the perspective of scanning RAM is taken throughout this thesis.

⁷⁹ Nick Cano, *Game Hacking: Developing Autonomous Bots for Online Games* (No Starch Press 2016) 270-271

a way to check for any modification, such as function hooks or pieces of injected code.⁸⁰⁸¹ Furthermore, it is also possible for gaming companies to **call a list of all the currently active windows and processes** on the user's computer.⁸²⁸³ Both have the potential to be quite invasive: window titles, for example, could theoretically reveal sensitive information about a person. It should be noted that game companies can apply techniques to minimize the privacy intrusion. For example, game companies could code their anti-cheat in such a way as to compare hashed values rather than comparing the window titles' actual names.⁸⁴

'A hash value (or simply hash), also called a message digest, is a number generated from a string of text. The hash is substantially smaller than the text itself, and is generated by a formula in such a way that it is extremely unlikely that some other text will produce the same hash value.'
(webopedia.com)

In a regular scenario, acquiring the information targeted by the detection methods discussed above (meaning memory contents, window titles and running processes respectively) is done through calling functions inherent in the Windows Application Programming Interface (API).⁸⁵⁸⁶ For example, reading a specific process memory space is achieved through calling the function: 'ReadProcessMemory'.⁸⁷ Having to use the Windows API also carries with it restrictions, however. The scope of such functions depends heavily on security permissions granted by the operating system (and thus the user, who is ultimately in control of the operating system).⁸⁸⁸⁹ In Windows, some processes are elevated

⁸⁰ *Ibid*

⁸¹ Interview with participant #1 (Through e-mail, February 2017) 82-84

⁸² Chris Hogg and Gary McGraw, *Exploring Online Games: Cheating Massively Distributed Systems* (Kindle Edition, Second Printing, Pearson Education 2008) Location 476

⁸³ Interview with participant #2 (Skype, February 12 2017) 86-87

⁸⁴ Whether and to what extent such techniques are actually being used is, of course, unknown, as game companies do not disclose this.

⁸⁵ See: [https://msdn.microsoft.com/nl-nl/library/windows/desktop/ff818516\(v=vs.85\).aspx](https://msdn.microsoft.com/nl-nl/library/windows/desktop/ff818516(v=vs.85).aspx) (Microsoft Developer Network Documentation)

⁸⁶ Interview with participant #1 (Through e-mail, February 2017) 83

⁸⁷ See: [https://msdn.microsoft.com/nl-nl/library/windows/desktop/ms680553\(v=vs.85\).aspx](https://msdn.microsoft.com/nl-nl/library/windows/desktop/ms680553(v=vs.85).aspx) (Microsoft Developer Network Documentation)

⁸⁸ *Ibid*

⁸⁹ Interview with participant #1 (Through e-mail, February 2017) 83; Interview with participant #2 (Skype, February 12 2017) 86-87

(administrator-level) while others are not (standard-level).⁹⁰ If a non-elevated process tries to call ReadProcessMemory and targets an elevated process, Windows will not allow it.⁹¹ So, if a cheater is able to ensure that the anti-cheat software runs at standard-level while the cheating software runs at administrator-level, gaming companies cannot scan that memory space (see figure 2). But there are ways around this. In Windows and most other operating systems, code can be executed in either *user mode* or *kernel mode*.⁹² In user mode, code cannot directly access devices or system memory but must do so through calling the Windows API. This is the default mode of operation: it is more restrictive (which from the user's perspective is a good thing) but errors or crashes in user mode do not tend to be fatal (meaning total system shutdown). In kernel mode, on the other hand, code has complete and direct access to hardware and any memory space. It does not need to call Windows API functions and is thus free from its restrictions.^{93,94} It is for this reason that some anti-cheat software applications opt to run in kernel-mode (see figure 3).⁹⁵ To complicate matters further, cheating software can also opt to run in kernel-mode. Discussing exactly what this all means for detection is too theoretical (most of it would be conjecture) and beyond the scope of this thesis. It is merely important to know that, regardless of the specifics of the situation, anti-cheating

'In Kernel mode, the executing code has complete and unrestricted access to the underlying hardware. It can execute any CPU instruction and reference any memory address. Kernel mode is generally reserved for the lowest-level, most trusted functions of the operating system. Crashes in kernel mode are catastrophic; they will halt the entire PC.'
(codinghorror.com)

⁹⁰ See: [https://msdn.microsoft.com/en-us/library/windows/desktop/aa379306\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/aa379306(v=vs.85).aspx) (Microsoft Developer Network Documentation)

⁹¹ See: [https://msdn.microsoft.com/nl-nl/library/windows/desktop/ms680553\(v=vs.85\).aspx](https://msdn.microsoft.com/nl-nl/library/windows/desktop/ms680553(v=vs.85).aspx) (Microsoft Developer Network Documentation)

⁹² See: <https://msdn.microsoft.com/en-us/windows/hardware/drivers/gettingstarted/user-mode-and-kernel-mode> (Microsoft Developer Network Documentation)

⁹³ *Ibid*

⁹⁴ Interview with participant #2 (Skype, February 12 2017) 88-90

⁹⁵ Interview with participant #1 (Through e-mail, February 2017) 83

software under kernel mode is more capable of detecting cheats. However, it is not absolutely required: even in the situation where the cheat does run in kernel mode, detection is possible but may require game companies to think outside of the box and spend time and effort developing creative solutions, rather than employing conventional methods of detection.⁹⁶ For example, it was recently discovered that Valve was **investigating players' dns-caches** (something comparable to a browser history), searching for any connections with known digital rights management servers associated with commercial cheat software.⁹⁷ Indeed, as Gabe Newell, CEO of Valve has stated in the past, '*kernel-level cheats are expensive to create, and they are expensive to detect.*'⁹⁸

To summarize, conventional methods of detection rely predominantly on memory reading or calling certain functions through the Windows API. Whether these functions have (full) access to the memory beyond the space inhibited by the game itself depends on security privileges granted by the operating system. One way of circumventing these restrictions is executing anti-cheat software code in kernel mode. This grants anti-cheat full access to the entire computer. Another way is developing specific detection techniques that look for changes caused by cheats in the user environment, rather than the cheats themselves.

Client-side anti-cheat (overview)

- Binary validation
- Signature based detection
- Screenshots
- Enumerating window titles and processes
- DNS-cache scanning
- Engaging kernel-mode

⁹⁶ Such cheats still affect the user space environment by, for example, creating new files or registry entries. See: Thomas Curda, 'Analysis and detection of online game cheating software' (Bachelor thesis, Masaryk University 2004) 37

⁹⁷ Peter Bright, 'Valve DNS privacy flap exposes the murky world of cheat prevention' (Ars Technica, 18 February 2014) <<https://arstechnica.com/gaming/2014/02/valve-dns-privacy-flap-exposes-the-murky-world-of-cheat-prevention/>> accessed on 2 February 2017

⁹⁸ Quoted from: www.reddit.com/r/gaming/comments/1y70ej/valve_vac_and_trust/

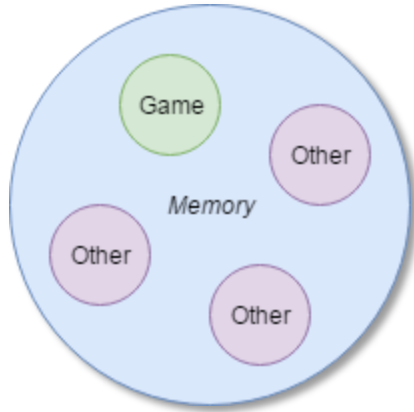


Figure 1

The typical scenario where no cheats or cheat detection are taking place. The memory space inhibited by the game is undisturbed and it does not invade any other memory spaces beyond its own.

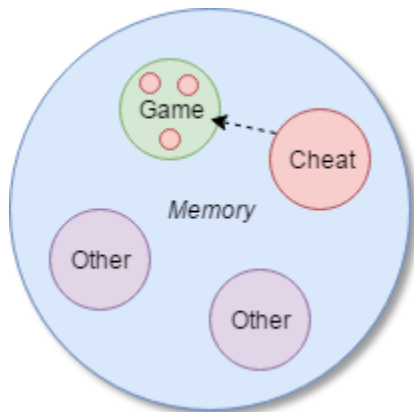


Figure 2

Here, a cheat (signified by red) is being employed by the user. The cheat invades the memory space inhibited by the game. The game/anti-cheat, however, does not or cannot cross the memory boundary. Detection is possible, but only by detecting forbidden activity inside the memory space inhibited by the game itself.

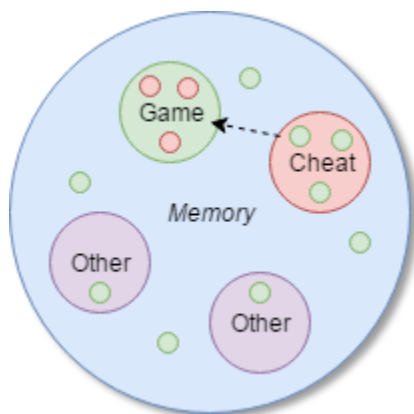


Figure 3

Here, a cheat (signified by red) is also being employed by the user and it invades the memory space inhibited by the game. Contrary to figure 2, the anti-cheat (signified by green) crosses the memory boundary and invades the user's entire memory space in search of cheats.

2.10.2 Server-side detection methods

Whereas client-side detection methods seek to identify cheats on a technical level, server-side detection relies on comprehensive analysis of player-behavior. Server-side detection methods have gained popularity in recent years and are the primary focus with regards to bot detection in academic writings.⁹⁹¹⁰⁰

Many writings proposing new methods of server-side detection simultaneously criticize client-side detection methods and their proposed methods as less invasive and more effective.¹⁰¹ Other authors describe server-side detection as easily circumventable.¹⁰² In line with the old adage that the truth is usually somewhere in the middle, I argue that server-side methods are effective at catching botters but not quite the end-all solution as they may appear at first glance. One reason for that is that server-side analysis requires significant processing power which may significantly dampen its theoretical potential.¹⁰³¹⁰⁴ Furthermore, it is impossible to know exactly how effective server-side analysis is in the grand scheme of things as one never knows how many bots evaded the analysis. So, while some authors argue, for example, that their analysis-scheme reaches a 95% detection ratio, such ratios are achieved in an experimental setting and are tested against lists of botters already identified by the game company.¹⁰⁵ Indeed, if server-side detection methods were truly that effective, it stands to reason that client-side detection methods would have been long abandoned by game-developers and that botting was no longer such a problem – both of which have not happened. Ironically, publishing academic articles further

⁹⁹ A quick search on Google Scholar or similar platforms reveals that almost all the articles have to deal with server-side detection. Client-side detection is only rarely mentioned.

¹⁰⁰ It is less relevant for detection of cheats used individually by active players. Bots revolve around the concept of automation, which is why behavioral analysis is effective at detecting them. Individual cheats used by active players (the ability to see through walls, for example) is much less likely to result in behavioral changes that can be identified by an algorithm.

¹⁰¹ See, for example: Chung and others, ‘A Behavior Analysis-Based Game Bot Detection Approach Considering Various Play Styles’ (2013) 35(6) ETRI Journal 1058, 1058-1059; Kang and others, ‘Multimodal game bot detection using user behavioral characteristics’ (2016) 5 SpringerPlus 523; Mitterhofer and others, ‘Server-Side Bot Detection In Massively Multiplayer Online Games’ (2009) 7(3) IEEE Security & Privacy 1, 2

¹⁰² Nick Cano, *Game Hacking: Developing Autonomous Bots for Online Games* (No Starch Press 2016) 286-287

¹⁰³ Chung and others, ‘A Behavior Analysis-Based Game Bot Detection Approach Considering Various Play Styles’ (2013) 35(6) ETRI Journal 1058, 1058-1059

¹⁰⁴ See also: Interview with participant #2 (Skype, February 12 2017) 92

¹⁰⁵ See, for example: Kang and others, ‘Multimodal game bot detection using user behavioral characteristics’ (2016) 5 SpringerPlus 523, 527

undermines the future potential of such detection methods as they are freely available to bot developers who will undoubtedly use them to educate themselves and evade detection.¹⁰⁶

2.11 Conclusion

In conclusion, the virtual worlds of online gaming can be both entertaining and profitable and this is reason for many to break the rules. Cheating and cheat detection are not only technologically complex but also actively obfuscated by the respective parties due to strong interests in secrecy. Furthermore, while the perspective of a strict separation between the real world and virtual world is alluring, (anti-)cheat is a prime example of how this dichotomy is an illusion. Several types of anti-cheat exist, but client-side techniques in particular reach far beyond the virtual realm of the game itself as they scan and investigate the user's computer. The next logical step is therefore to assess the legality of such methods.

¹⁰⁶ See, for example: <https://forums.tibiawindbot.com/showthread.php?18120-Bot-Detection-Article>

CHAPTER THREE – THE LAWFULNESS OF CLIENT-SIDE ANTI-CHEAT

3.1 Introduction

With the technological background sufficiently explored, this thesis now turns its attention to the legal implications of client-side anti-cheat. By now, it has become clear that the technological concepts from chapter two relate to privacy and data protection rights in at least some form or another. In order to understand how the law restricts game companies' in their application of client-side anti-cheat, further conceptualizing and analyzing that relationship is imperative.

Chapter three will follow the following structure. First, it will be made clear how client-side anti-cheat implicates privacy and data protection rights and how these implications dictate the choice in legal instruments for analysis. I will then show how Article 5(3) of the ePrivacy Directive, which protects end-users terminal equipment from interference, is applicable to the case of client-side anti-cheat. Building on this, I will argue that game companies can, at least in the case of scanning the memory space occupied by the game itself, circumvent the requirement of consent through the exceptions provided for in Article 5(3). This does not hold for any detection that crosses the memory boundary, however. Such detection must meet the requirement of informed consent, which must be placed and understood in the appropriate context.

3.2 The implications to privacy and data protection

Privacy is a multifaceted concept which protects many different interests but is at the same time difficult to define.¹⁰⁷ While a commonly accepted definition remains elusive, it is clear that the right to respect for private and family life entails several components, one of which is the right to informational privacy – the control of information about oneself.¹⁰⁸¹⁰⁹ And it is this aspect of privacy in particular which is implicated via client-side anti-cheat. As I have shown in chapter two, such anti-cheat by definition takes place on the user's computer. Computers – and other

¹⁰⁷ Daniel J Solove, 'Conceptualizing Privacy' (2002) 90(4) California Law Review 1087

¹⁰⁸ *Ibid*, 1125

¹⁰⁹ This component of privacy is often equated to data protection. Although the two share a close relationship, they are not identical. Data protection provides protection regardless of whether the right to respect for private life is implicated. See: Peter Hustinx, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation' (2013) Collected Courses of the European University Institute's Academy of European Law (24th Session on European Union Law), 50

devices like it – have the potential to (and often do) contain vast amounts of information about our personal lives. Credit-card numbers, browser histories, private conversations, embarrassing photographs, these are just a few examples. To quote one of the US Supreme Court Justices, ‘with all they contain and all they may reveal, they hold for many (...) “the privacies of life”’.¹¹⁰¹¹¹ Indeed, a brief look into someone’s phone or computer is likely to reveal more than a thorough search of someone’s entire house.¹¹² It is therefore not surprising that the European Union considers such devices to be part of the private sphere, ‘requiring protection under the Charter of Fundamental Rights and the European Convention for the Protection of Human Rights and Fundamental Freedoms’.¹¹³

Client-side anti-cheat may very well come into contact with our ‘privacies of life’. In 2005, a computer scientist by the name of Chris Hوجلund became well known in the gaming community for his technical research into Warden, anti-cheating software created and employed by Blizzard Entertainment, developer and publisher of the popular massive multiplayer online game ‘World of Warcraft’. According to Hوجلund, ‘Warden (...) uses the *GetWindowTextA* function to read the window text in the title bar of every window. These are windows that are not in the World of Warcraft process, but any program running on your computer. (...) I really believe that reading these window titles violates privacy, considering window titles contain a lot of personal data.’¹¹⁴ In his book, he argues that Warden and other software like it should be classified as spyware.¹¹⁵ The Electronic Frontier Foundation calls it a ‘massive invasion of privacy’.¹¹⁶ Others have expressed similar concerns.¹¹⁷¹¹⁸ Taking into consideration the full

¹¹⁰ Riley v. California, No. 13-132, 573 U.S. ____ (Supreme Court of Justice, 2014) 28

¹¹¹ Although the Court is talking about cell phones, the statement is equally (if not more) applicable to computers or other terminal devices.

¹¹² Riley v. California, No. 13-132, 573 U.S. ____ (Supreme Court of Justice, 2014) 21

¹¹³ Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) [2017] (COD) Recital 20

¹¹⁴ Chris Hوجلund and Gary McGraw, *Exploring Online Games: Cheating Massively Distributed Systems* (Kindle Edition, Second Printing, Pearson Education 2008) Location 1593

¹¹⁵ *Ibid*, 1559

¹¹⁶ Corynne McSherry, ‘A New Gaming Feature: Spyware’ (*Electronic Frontier Foundation*, October 20 2005) <www.eff.org/nl/deeplinks/2005/10/new-gaming-feature-spyware> accessed 3 March 2017

¹¹⁷ Rahul Joshi ‘Cheating and Virtual Crime in Massively Multiplayer Online Games’ (Master thesis, University of London 2008) 59

¹¹⁸ Establishing the accuracy of these claims for Warden specifically is beyond the scope of this thesis. I will say, however, that Hوجلund’s reverse engineering of the Warden software, on which many of the claims by other authors

spectrum of invasiveness, one could even say that the intrusion of analyzing window titles is still relatively tame. On the far side of the spectrum, anti-cheat that operates in kernel-mode has full access to the user's computer, which includes window titles, running processes, hard-drive contents, browser histories, hardware information, and so forth, containing an amount of personal information of which even the user himself is unlikely to be fully aware.

Those sympathetic to such business practices – which are after all in pursuit of a legitimate aim – may argue that no real invasion of privacy need necessarily occur. Companies with honest intentions will ask for consent, and are only looking at a specific subset of information. The problem with this argument is that it relies on complete faith in the game company to provide users with the appropriate information prior to consent, to not overstep its boundaries and to understand where these boundaries lie in the first place.¹¹⁹ Such faith can reasonably only exist if a significant degree of transparency is present, and, as I will show, it is exactly transparency that is lacking in this context. Solove argues similarly and calls attention to the fact that privacy harms lie not only in concrete adverse consequences, but other problems such as vulnerability and exclusion created by a lack of transparency and accountability.¹²⁰ The problem is not that every game company will act dishonestly or overstep its bounds in ignorance. Rather, the concern is that the potential for intentional and unintentional abuse is always present – the user's '*privacies of life*' are exposed and vulnerable, one miss-step away from being inappropriately viewed, out of his or her control. Building on this, it becomes clear that the implication for privacy lies not (exclusively) in the content of the exposed information but rather the collection process as a whole.

Because anti-cheat is a technologically complex subject with which most readers are likely to be unfamiliar, further concretizing the privacy concern may be helpful. In his work on conceptualizing privacy, Solove emphasizes the value of analogical reasoning when identifying

are based, do not show exactly (among other things) which information is being sent back to Blizzard Entertainment. In my view, this is something that should at least be fully investigated before labeling a piece of software as actual spyware, which is, after all, a serious accusation. I would therefore urge other authors to critically assess his findings and make up their own minds before using it as a basis for further research.

¹¹⁹ What is meant here is that game companies may very well be unaware of where the legal limits lie. Cheat detection is a legal gray area which has remained relatively unexplored by legal scholars.

¹²⁰ Daniel J Solove, "'I've Got Nothing to Hide'" and Other Misunderstandings of Privacy' (2002) 44(1) San Diego Law Review 745, 758-759

privacy concerns.¹²¹ Two such analogies can be made here. First of all, there is a clear parallel to state surveillance, with game companies taking the role of the state, cheaters taking the role of law-breaking citizens and legitimate players taking the role of law-abiding citizens. Notions of powerlessness and a lack of transparency and accountability are key here.¹²² Completing the analogy, some users with a particular distaste for cheating have gone as far as to raise the ‘nothing to hide’ argument.¹²³ While I will not deconstruct that particular argument here, its presence further emphasizes the similarities to the situation of government surveillance and helps us to better envision the way in which privacy is implicated in the case of anti-cheat. The second analogy to be made is less concrete but nevertheless enlightening. While we are dealing with informational privacy, there also seems to be an element of spatial privacy at play. Our computers, similar to our houses, contain a vast amount of potentially sensitive information and are part of the private sphere. If we invite a mechanic into the house to fix the kitchen sink, we would not want to find him digging around in our bedroom. In the same vein, certain memory *spaces* are accessible to the game company (in particular those necessary to enable the service) while others are strictly off-limits barring our clear consent. Intrusions into this space, regardless of which information is accessed, by whom, or in what way, are in themselves privacy violations and must be treated accordingly.

This line of argumentation is essentially embodied by Article 5(3) of the Privacy and Electronic Communications Directive (henceforth: ePrivacy Directive), which holds the terminal equipment of the user to be part of the private sphere and only allows access to information therein – *regardless of content* – when informed consent is present.¹²⁴ The European Commission describes the rationale underlying Article 5(3) as being ‘*based on the understanding that the terminal equipment is part of the private sphere of an individual, **in the same way as his or her domicile and communications***’.¹²⁵ While the Directive acts as a *lex specialis* to the Data Protection Directive and is limited in scope to data processing ‘*in connection with the provision*

¹²¹ *Ibid*, 759

¹²² Parliament and Council Directive 2002/58/EC of 12 July 2 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37 art 5(3)

¹²³ See, for example: <https://us.battle.net/forums/en/wow/topic/17597549585>

¹²⁴ In other words, regardless of whether it constitutes personal data or not.

¹²⁵ European Commission, ‘Ex-Post REFIT evaluation of the ePrivacy Directive 2002/58/EC’ (Commission Staff Working Document, 2017)

of publicly available electronic communications services in public communications networks’, Article 5(3) is an article of general provision and extends beyond this scope.¹²⁶¹²⁷ Because any information extracted via methods of client-side anti-cheat must by definition originate from the user’s terminal equipment, the ePrivacy Directive is the logical instrument of choice in assessing the legality of such methods. Furthermore, although Article 5(3) is predominantly a privacy protection mechanism, data protection legislation specifically also comes into play in two different ways. First, if the information collected constitutes personal data, the GDPR becomes applicable in its entirety. It is important to note, however, that this does not mean that the other lawful processing grounds enumerated in Article 6 of the GDPR can be relied upon to collect the personal data; any collection from the end-user’s terminal equipment must *always* be based on Article 5(3). Second, the ePrivacy Directive and the proposed ePrivacy Regulation both define the notion of consent by referring to the Data Protection Directive (DPD) and GDPR respectively. Interpreting the meaning of consent in the context of the ePrivacy Directive will therefore require incorporating these legal instruments into the analysis as well.¹²⁸

3.3 A closer look at the applicability of the ePrivacy Directive

As discussed, Article 5(3) of the ePrivacy Directive is an article of general provision and extends beyond the normal scope of this Directive.¹²⁹¹³⁰ Article 5(3) is technologically neutral and is applicable not only to cookies but to any technology that gains access to or stores information on the end-user’s terminal equipment.¹³¹¹³² The type of information accessed is irrelevant with

¹²⁶ Information society services are explicitly excluded from the definition of ‘*electronic communications services*’ and therefore fall outside the scope of the ePrivacy Directive. Because online gaming companies offer a service which does not consist ‘*wholly or mainly in the conveyance of signals on electronic communications networks*’ (See Directive 98/34/EC, art 1), it indeed qualifies as an information society service. This means that, aside from Article 5(3), the ePrivacy Directive is not particularly relevant to the online gaming industry.

¹²⁷ Eleni Kosta, *Consent in European Data Protection Law* (Martinus Nijhoff Publishers, 2013) 293

¹²⁸ Focus will be on the GDPR as the DPD is quickly growing irrelevant. However, for the time being, the ePrivacy Directive still relies on the DPD for defining consent, which is why it will be referred to as well in the analysis. This will sometimes be done interchangeably.

¹²⁹ Parliament and Council Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37 art 5(3)

¹³⁰ Article 29 Working Party, ‘Opinion on online behavioral advertising, WP171’ (2010) 9

¹³¹ *Ibid.*, 8

regards to Article 5(3)'s applicability. All information – personal data or not – is protected.¹³³ The terms ‘*gaining access*’ and ‘*storing information*’ are not explicitly defined in legislation, which has raised questions as to the extent of its applicability.¹³⁴ However, there is sufficient evidence to support a wide interpretation that includes client-side anti-cheat. Recital sixty-six of Directive 2009/136/EC¹³⁵ recognizes that third parties may wish to gain access to information for malicious purposes and explicitly refers to spyware and viruses as examples of this. It characterizes spyware as ‘*software that surreptitiously monitors the actions of the user or subverts the operation of the user’s terminal equipment to the benefit of a third party*’.¹³⁶ Client-side detection methods have been likened to spyware in both mainstream discourse¹³⁷ and academia.¹³⁸ While not necessarily (but nevertheless quite possibly) malicious in the same way as spyware, client-side anti-cheat fits the characterization posed by Directive 2009/136/EC as it by definition monitors the actions of users. Whether this monitoring is surreptitious or not depends on whether the consent requirement in Article 5(3) is met. Furthermore, a proposal for an e-Privacy Regulation was made public by the European Commission just recently.¹³⁹ The proposal rephrases Article 5(3) in such a way that the legislator’s intent becomes much more clear: any use of the processing or storage capabilities of terminal equipment and the collection of information from end-users’ terminal equipment shall be prohibited unless the requirements

¹³² See also: Parliament and Council Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37, Recital 25

¹³³ Eleni Kosta, *Consent in European Data Protection Law* (Martinus Nijhoff Publishers, 2013) 297-298

¹³⁴ See: European Commission, ‘Ex-Post REFIT evaluation of the ePrivacy Directive 2002/58/EC’ (Commission Staff Working Document, 2017) 41

¹³⁵ Directive 2009/136/EC amends the ePrivacy Directive.

¹³⁶ Parliament and Council Directive 2009/136/EC of 25 November 2009 amending Directive 2002/22/EC on universal service and users’ rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws [2009] OJ337/11 Recital 66

¹³⁷ See: Mark Ward, ‘Warcraft game maker in spying row’ (BBC News, 31 October 2005) <<http://news.bbc.co.uk/2/hi/technology/4385050.stm>> accessed February 20 2017

¹³⁸ See: An Hilven and Andrew Woodward, ‘How safe is Azeroth, or, are MMORPGS a security risk?’ (Proceedings of The 5th Australian Information Security Management Conference, Perth 2007)

¹³⁹ Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) [2017]

are met.¹⁴⁰ Taking all of the above into account, concluding Article 5(3)'s applicability is justified.

3.4 Exceptions to Article 5(3)

Article 5(3) of the ePrivacy Directive allows for two situations in which consent is not required. The first exception allows for '*technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network*¹⁴¹', whereas the second exception allows for access '*as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user*'.¹⁴² With regards to the first exception, accessing the user's terminal equipment in order to detect cheats is clearly not required for the sole purpose of making the communication between client and server possible. The second exception, however, appears somewhat more salient. Online games fit the definition of information society services, as defined in Directive 98/34/EC.¹⁴³ Would it be possible to argue that accessing information on the user's terminal equipment in search of cheats is strictly necessary to the provision of such a service, as it is indeed the user who explicitly requests it?

Because legislation provides very little additional clarification, it is unclear how the term '*strictly necessary*' should be interpreted.¹⁴⁴ The Information Commissioner's Office (ICO) has stated that '*strictly necessary*' should be understood as '*essential rather than reasonably necessary*'.¹⁴⁵ Applicability of the exemption should also be limited '*to what is essential to provide the service requested by the user, rather than what might be essential for any other uses the service provider might wish to make of that data*'.¹⁴⁶ ICO therefore holds the exception to be narrow and strict.¹⁴⁷ In line with that interpretation, *strictly* implies the need for direct causality between the device (anti-cheat) and the service (the game and its features). However, client-side anti-cheat is not inseparably connected to providing the service because the game can be played

¹⁴⁰ *Ibid*, art 8

¹⁴¹ Parliament and Council Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37, art 5(3)

¹⁴² *Ibid*

¹⁴³ See also: Article 29 Working Party, 'Opinion 04/2012 on Cookie Consent Exemption, WP194' (2012) 2-3

¹⁴⁴ Eleni Kosta, *Consent in European Data Protection Law* (Martinus Nijhoff Publishers, 2013) 286-287

¹⁴⁵ Information Commissioner's Office, 'Guidance on the Privacy and Electronic Communications' (2012) 12

¹⁴⁶ *Ibid*

¹⁴⁷ *Ibid*

without it.¹⁴⁸ The fact that one of the most popular online massive multiplayer online games currently on the market supposedly does not rely on client-side anti-cheat at all further solidifies the conclusion that the exception under Article 5(3) does not apply.¹⁴⁹ But things appear to be changing. The European Commission is of the opinion that ‘*the consent rule to protect the confidentiality of terminal equipment failed to reach its objectives*’ due to being simultaneously under-inclusive (in the sense that not all tracking techniques are covered) and over-inclusive (in that it also covers non-privacy intrusive practices).¹⁵⁰¹⁵¹ The over-inclusivity mentioned by the Commission seems to be in part reflected by a subtle change to Article 5(3) (now Article 8) in the ePrivacy Regulation proposal: consent is not required if the access is ‘*necessary for providing an information society service requested by the end-user*’ rather than ‘*strictly necessary*’.¹⁵² Under this regime, it becomes more likely that client-side anti-cheat would fit the exception.¹⁵³ Rules are after all an important part of any game and it is not that far-fetched to claim that identifying rule violators is – while not *strictly* necessary – at least necessary in the broader sense of the word. Assuming this interpretation is correct, does this mean that game companies are free to use any method of detection as they see fit without having to ask for consent? It cannot. Such an assertion would be incompatible with the fact that terminal equipment is protected by the Charter and ECHR. Necessity implies proportionality: Recital 21 of the ePrivacy Regulation proposal states that ‘*for instance, consent should not be requested for*

¹⁴⁸ This would be like saying that checking passengers’ tickets (in other words, making sure passengers ‘play by the rules’) is necessary to power a train (in other words, to provide the service): it simply does not make sense from a direct causality perspective.

¹⁴⁹ The game which is being referred to is Final Fantasy 14. It cannot be said with 100% certainty that it does not incorporate client-side anti-cheat. However, Square-Enix is known as a very reputable company and does not incorporate any monitoring clauses in its terms as would normally be the case. There are also plenty of reports that cheaters and botthers tend to go unbanned for a long time, further reinforcing this suspicion. See:

www.reddit.com/r/ffxiv/comments/6bzahy/a_word_of_caution_about_asking_for_more/;

www.reddit.com/r/ffxiv/comments/4c5e11/suspended_guilty_current_specification_is_too/;

www.reddit.com/r/ffxiv/comments/1m4rx1/keep_an_eye_out_for_teleporting_botthers/

¹⁵⁰ Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) [2017] 5

¹⁵¹ While the proposal envisions many more changes and restructures the entire framework in a significant way, it is beyond the scope of this thesis to provide a comprehensive and in-depth analysis of that.

¹⁵² Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) [2017] art 8

¹⁵³ Confusingly, Recital 21 returns to the original terminology of ‘strictly necessary’, casting further doubts on the intention of the legislator.

*authorizing the technical storage or access which is strictly necessary **and proportionate** for the legitimate purpose of enabling the use of a specific service explicitly requested by the end-user'* (emphasis mine).¹⁵⁴ Furthermore, Recital 21 makes clear that exceptions to consent '*should be limited to situations that involve no, or only very limited, intrusion of privacy*'.¹⁵⁵ Given that terminal equipment belongs to the private sphere, and that some forms of detection have total, unbridled access to terminal equipment, the privacy intrusion cannot always be regarded as very limited. At most, the new regime would allow for consentless detection contained to the memory space inhibited by the game. Concluding differently would go against the rationale of the Article 5(3), which protects the user's terminal equipment – not necessarily because of the content of such information (after all, it is irrelevant whether the information constitutes personal data or not) or what companies decide to do with it – but rather the fact that any information on such equipment by definition belongs to the private sphere (similarly to someone's domicile). If companies are free to access whatever space they see fit without asking for consent as long as the act meets some broad requirement of necessity, the protections bestowed by the ePrivacy Directive and upcoming Regulation would be rendered effectively meaningless.

3.5 Circumventing the consent requirement

Cheat detection is not the only reason a game company may want to collect information from their users' computers. In line with the client-server architecture, gameplay is made possible through constant communication between the two entities. The server takes a leading role and collects information from the end-user by instructing the game software to send the appropriate information required to enable gameplay. The key difference with anti-cheat is that this will only concern information flowing from the memory space inhibited by the game itself. This concerns a service that was explicitly requested by the user, and any access, storage or collection in this context is therefore strictly necessary to enable the provision of said service and fits the exception under Article 5(3). However, as I have shown in chapter two, cheats influence the game memory space through code injection or function hooks. Binary validation and signature

¹⁵⁴ Confusingly, the legislator returns to the original terminology ('strictly necessary') here. It is unclear why this term was chosen whereas the word 'strictly' has been removed from Article 8.

¹⁵⁵ Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) [2017] recital 21

based detection methods do not necessarily require access to information beyond the memory space inhabited by the game in order to be effective. From the game company's perspective, it may be quite interesting to determine whether information collected under Article 5(3)'s '*strictly necessary*' exception can be re-used for anti-cheat, thus effectively bypassing the need to obtain consent. I argue that this is indeed possible. With regards to binary validation, actual code on the user's terminal equipment is compared to an original 'clean' version. Verifying the integrity of the game cache is on the one hand necessary in order to facilitate gameplay, as the code running on the client-side must be devoid of bugs, memory corruptions and other serious abnormalities. On the other hand, it may simultaneously also reveal intentional modification via memory writing, function hooks, or other cheat-techniques. Binary validation is therefore legally not problematic as cheat detection is a convenient side-effect resulting from a collection which is necessary for the provision of the service. With signature based detection, however, code excerpts are compared to a blacklist of known byte patterns associated with cheat software. In this case, cheat detection is not a convenient by-effect but rather a deliberate additional step which is applied to the information collected originally for an entirely different purpose. The question then becomes whether the processed information, essentially bits of computer-code, constitute personal data or not. If it is indeed personal data, then this second purpose must be compatible with the original purpose.¹⁵⁶ If it is merely information, then it stands to reason that game companies can re-use that information however they see fit. This topic, however, is beyond the scope of this thesis and has been suggested as a possible area for future research (see 6.2).

3.6 Informed consent

In any case, although using information originating from the memory space inhabited by the game for cheat detection is not legally problematic, accessing information beyond that boundary, is. Neither exception in Article 5(3) can be invoked in order to circumvent the requirement of informed consent. Seeing as how Article 5(3) provides no other lawful grounds for accessing the user's terminal equipment, investigating beyond the memory space inhabited by the game must by definition be based on informed consent.

¹⁵⁶ ¹⁵⁶ Parliament and Council Regulation of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ 119/1, art 5

3.6.1 The content of the information

The e-Privacy Directive states that access to *‘the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing’*.¹⁵⁷ Similarly, the e-Privacy Regulation proposal provides that the definitions and conditions of consent shall be in line with Articles 4(11) and 7 of the GDPR. With regards to information to be given to the data subject, the GDPR only mentions a few types of information, none of which directly relate to the implications and consequences of client-side anti-cheat.¹⁵⁸ One could argue that there is thus no problem at all: game companies are not obligated to disclose any further information related to cheat detection as long as the purpose (‘cheat detection’) is made sufficiently clear. But this interpretation cannot hold. The choice by the legislator to define consent under the ePrivacy Directive/Regulation by simply ‘importing’ consent from the DPD/GDPR is problematic because it fails to recognize that Article 5(3) deals with an entirely different situation: what is at stake here is not (only) the processing of personal data, but rather the way in which *information* is collected through accessing a user’s terminal equipment. As such, I argue that the interpretation of what constitutes informed consent should be modified accordingly. The Article 29 Working Party has stated that *‘consent by the data subject (must be) based upon **an appreciation and understanding of the facts and implications of an action**. The individual concerned must be given, in a clear and understandable manner, accurate and **full information of all relevant issues, in particular those specified in Articles 10 and 11 of the Directive’*** (emphasis mine).¹⁵⁹ Taking the above into account, it becomes clear that the information which needs to be provided in order for a user to be sufficiently informed is dependent on which particular action a user is consenting to. Indeed, as has also been recognized in the literature, *‘the quality and quantity of [the] information must be proportional to the risks associated with the particular data-*

¹⁵⁷ Parliament and Council Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37, art 5(3)

¹⁵⁸ Parliament and Council Regulation of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ 119/1, art 13

¹⁵⁹ Article 29 Working Party, ‘Opinion 4/2007 on the definition of consent, WP187’ (2011) 19

processing operation for which consent is sought.¹⁶⁰ While it is true that Article 13 of the GDPR – which enumerates the information to be given prior to collection from the data subject – is often associated with what it means in order for consent to be informed, is seemingly exhaustive and makes no mention of the way in which data is accessed or processed, the legislator does not state anywhere state that the elements in Article 13 are to be the sole foundation of informed consent.¹⁶¹ On the contrary, Recital 62 of the GDPR states that the data subject should be provided with ‘*any further information necessary to ensure fair and transparent processing*’. In summary, because consent under Article 5(3) of the ePrivacy Directive sees to an entirely situation than the one normally covered under the DPD and GDPR, the informational requirements must be modified in line with that contextual shift. Not doing so would mean that, for example, the use of invasive anti-cheat that operates on the kernel-level (with unbridled access to the user’s memory and hard-drive contents and any other hardware as a result) would be lawful via informed consent, merely because the user was informed of the fact that his or her terminal equipment may be accessed for ‘cheat detection’. Seeing as how the ePrivacy Regulation proposal explicitly considers the terminal equipment of the end-user to be part of the private sphere and thus under protection of the Charter of Fundamental Rights of the European Union, such a restrictive interpretation of informed consent cannot hold.¹⁶² In order for data subjects to be sufficiently informed, game companies must disclose not only broadly defined purposes but also more detailed information concerning the ways in which the user’s terminal equipment will be accessed and how. As Barnes succinctly puts it in his work on spyware-contracts, ‘*without such a description of what the software is actually going to do, contract and other law has little difficulty concluding that any access and surveillance would be unauthorized*’.¹⁶³ I speculate that the above does not follow directly and unambiguously from the legal text because it is almost always cookies that take center stage in the debate surrounding the protection of the end-user’s terminal equipment. Cookies, in comparison to some of the harder-

¹⁶⁰ Lee A Bygrave and Dag Wiese Schartum, ‘Consent, Proportionality and Collective Power’ in Gutwirth and others (eds) *Reinventing Data Protection?* (Springer Science Business Media 2009) 164

¹⁶¹ See, for example: Eleni Kosta, *Consent in European Data Protection Law* (Martinus Nijhoff Publishers, 2013) 204

¹⁶² Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) [2017] Recital 20

¹⁶³ Barnes W, ‘Rethinking Spyware: Questioning the Propriety of Contractual Consent to Online Surveillance’ (2006) 39 U.C. Davis Law Review 1545, 1604

hitting devices discussed in this thesis, are relatively innocent and consequently require less explanation as to its implications. Merely informing users of the intended purpose (e.g. tracking your behavior for marketing purposes) will often cover the necessary subject matter in order for end-users to be able to make an informed decision. The user has greater control because the pool from which information and personal data can be drawn is limited in scope to browser-activity. On the other hand, the ‘heavy-hitters’ may have access to the entire computer, in which a huge amount of information (and consequently also personal data) will be present.

3.6.2 The way in which the information is provided

To establish informed consent, information must also be provided in a clear and comprehensive way.¹⁶⁴ In the Article 5(3) context, this is often done through privacy policies or similar notices.¹⁶⁵¹⁶⁶ Anyone familiar with such agreements will know they are often long, convoluted and difficult to understand. Such problems also manifest in the case of spyware.¹⁶⁷ Users may be misled into installing spyware alongside other software by hiding such information deep in the terms of service.¹⁶⁸ Users accept the terms through click-wrap and check a box to signify their acceptance of the terms. While controversial, their validity is usually accepted in the European Union as long as the terms are clearly visible and presented to users.¹⁶⁹ Nevertheless, this does not mean that click-wrap agreements are beyond reproach and enforceable in every situation. In case law, enforceability tends to come into question particularly when the authoring party of the click-wrap agreement has taken steps or techniques to obfuscate the information therein.¹⁷⁰ To quote one author, ‘*spyware purveyors hide behind the line of click-wrap cases that look only to objective intent (...) [and] courts should not find genuine assent merely because (objectively) a*

¹⁶⁴ Eleni Kosta, *Consent in European Data Protection Law* (Martinus Nijhoff Publishers, 2013) 310

¹⁶⁵ *Ibid*, 215

¹⁶⁶ See also: Article 29 Working Party, ‘Opinion 4/2007 on the definition of consent, WP187’ (2007) 3

¹⁶⁷ Alan F Blakley, Daniel B Garrie and Matthew J Armstrong, ‘Coddling Spies: Why The Law Doesn’t Adequately Address Computer Spyware’ (2005) 25(1) *Duke Law & Technology Review*

¹⁶⁸ *Ibid*, 9

¹⁶⁹ Reinoud Westerdijk, ‘The Evolution and Transformation of IT Contracting and Outsourcing Over 4 Decades Software Delivery: From Shrink-Wrap to the Cloud and Beyond’ (World Technology Law Conference & Annual Meeting, San Francisco 2011)

¹⁷⁰ Mathias Klang, ‘Spyware: paying for software with our privacy’ (2010) 17(3) *International Review of Law, Computers & Technology* 313, 316

button was clicked.¹⁷¹ On the other hand, from the perspective of the controller, particularly in an online context, it is essentially impossible to be absolutely certain that the data subject has been sufficiently informed.¹⁷² Many users simply do not read terms of service, end user license agreements or privacy policies.¹⁷³ So how much responsibility should be ascribed to and expected from data subjects on the one hand and controllers on the other?¹⁷⁴ Recital 66 of Directive 2009/136/EC¹⁷⁵ stipulates ‘*methods of providing information (...) should be as user-friendly as possible*’.¹⁷⁶ The Article 29 Working Party, with regards to cookies, has stated that it is important ‘*for information to be easily accessible and highly visible*’.¹⁷⁷ Furthermore, ‘*(...) essential information may not be hidden in general terms and conditions and/or privacy statements*’¹⁷⁸. When we consider that the Article 29 Working Party’s statements concerned cookies, which, as discussed, are generally much less invasive than anti-cheat devices, it becomes clear that hiding provisions related to anti-cheat is at least equally if not more problematic.

3.7 Informed consent in practice

In order to further concretize the theoretical considerations and notions discussed in the previous paragraph, fifteen popular online games and three third-party anti-cheat software applications were investigated with regards to the content of the information they provide and the way in which they provide it.

¹⁷¹ Jordan Blanke, ‘“Robust Notice” and “Informed Consent:” The Keys to Successful Spyware Legislation’ (2006) 7(2) *The Columbia Science and Technology Review* 1, 15

¹⁷² Eleni Kosta, *Consent in European Data Protection Law* (Martinus Nijhoff Publishers, 2013) 217

¹⁷³ Stacey Higginbotham, ‘People trust the internet but lie to it anyway’ (Gigaom.com, November 27 2012) <<https://gigaom.com/2012/11/27/people-trust-the-internet-but-lie-to-it-anyway/>> accessed March 9 2016

¹⁷⁴ Eleni Kosta, *Consent in European Data Protection Law* (Martinus Nijhoff Publishers, 2013) 215

¹⁷⁵ Also known as the Citizens’ Rights Directive.

¹⁷⁶ Parliament and Council Directive 2009/136/EC of 25 November 2009 amending Directive 2002/22/EC on universal service and users’ rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws [2009] OJ337/11, Recital 66

¹⁷⁷ Article 29 Working Party, ‘Opinion 02/2010 on online behavioural advertising’, WP171’ (2010) 18

¹⁷⁸ *Ibid*

3.7.1 Findings (content)

Most online games and all third party anti-cheat make clear that the user may be monitored for purposes related to cheating in some way or another (terminologies include, ‘*unauthorized third party programs*’ and ‘*fraud*’). For the two online games that do not, one likely does not use client-side anti-cheat at all (Final Fantasy 14)¹⁷⁹ whereas the other game, Path of Exile, allegedly uses client-side anti-cheat¹⁸⁰, but does not mention this anywhere. Out of the remaining online games, around half specify that the user’s RAM may be monitored, whereas only Blizzard Entertainment threads into greater detail by enumerating other types of techniques which may be used. The (alleged) biggest offender is Black Desert Online, which uses XIGNCODE 3, anti-cheat developed in Korea which exhibits malware-like behavior.¹⁸¹ The software allegedly scans the user’s entire computer, operates on the kernel level and takes active control of the user’s PC by forcefully closing certain applications¹⁸², but the terms and conditions suggest or imply nothing of the sort. Finally, while third-party anti-cheat applications always make mention of particular techniques which may be used, none of them inform the user that they run in kernel-mode or the implications thereof.

3.7.2 Findings (conveyance)

With regards to the way in which the information is provided, information related to anti-cheat either appears in the privacy policy or terms of use. For online games, anti-cheat provisions are hidden and very difficult to find because they are obfuscated by long, convoluted lists of terms. Further, terminology used between games is inconsistent which makes searching for specific keywords difficult. Several online games do improve visibility by including an indexation at the start of the document which explicitly links to the location of the anti-cheat provisions. Anti-

¹⁷⁹ See footnote 149.

¹⁸⁰ See: <http://www.ownedcore.com/forums/mmo/path-of-exile/poe-bots-programs/508787-warning-anti-cheat-implemented-stop-using-any-hack-bot-proof-inside.html>

¹⁸¹ Aside from the large amount of reports by users, the company’s website indeed implies the presence of such functionality: <http://www.wellbia.com/home/en/pages/xigncode3/>

¹⁸² <https://steamcommunity.com/app/582660/discussions/0/1290691308571849109/?ctp=20>

cheat provisions in Blizzard Entertainment's games are the most visible as they provide a separate document titled 'Anti-cheat agreement'.¹⁸³

3.7.3 An example of questionable terms

The ESEA client is a software application that allows players access to specialized game servers on which the ESEA anti-cheat technology is active.¹⁸⁴ With regards to its anti-cheat functionality, the privacy policy is extremely ambiguous (see footnote).¹⁸⁵ The provision allows for complete access into the user's PC, as long as ESEA deems it 'reasonably necessary'. Perhaps even more concerning is a more recent addition to its functionality: capability to run even when the game is not running. It is not surprising that there are significant privacy concerns within the community over what exactly ESEA is collecting when the game is off and why.¹⁸⁶ Even more so when we consider that ESEA has already been caught sneaking malware (that forced users to unknowingly mine bit coins) into the client in the past.¹⁸⁷ In response to the always-on functionality, one player posed the following question to ESEA co-founder Eric Thunberg: '*So can you tell us without a doubt that this new client is trustworthy and will in no way do any malicious activity with our private files?*'.¹⁸⁸ Thunberg, clearly to the community's annoyance, responds: '*No, the only certainty in life is death*'.¹⁸⁹ Whatever the case may be, the average user who installs the software is unlikely to be aware of these issues based on the information provided in the privacy

¹⁸³ For third-party anti-cheat software, provisions are generally visible due to the fact that the privacy policies and terms on these websites need not feature anything else (as opposed to online games where anti-cheat is only a small part of the service/software package).

¹⁸⁴ See: <https://play.esea.net/index.php?s=support&d=faq>

¹⁸⁵ '*Certain information regarding your computer and software it contains is required for effective operation of our anti-cheat services. By using the ESEA Client, you consent to the collection and analysis of information from your computer that ESEA deems reasonably necessary to identify and prevent the use of cheat software, files used to gain an unfair advantage, and to enforce bans. This information collection is not strictly limited to when you are logged in to the ESEA Client. Information analyzed or collected by the ESEA Client may include hardware, network and software identifiers; running programs; system configuration information; files or data suspected of being used to cheat or gain an unfair advantage; or screenshots while you are logged in and playing a game through the ESEA Client*' Quoted from: https://play.esea.net/index.php?s=content&d=privacy_policy

¹⁸⁶ See, for example: https://www.reddit.com/r/GlobalOffensive/comments/36o0c9/boycott_esea/;
www.reddit.com/r/GlobalOffensive/comments/36inncc/esea_client_update_questions_for_lpkane/;
www.hltv.org/forum/799316-esea-client-now-quotalways-onquot

¹⁸⁷ Aaron Souppouris, 'Employee creates Bitcoin botnet to exploit ESEA's 500,000-member gaming community' (The Verge, May 2 2013) <<http://www.theverge.com/2013/5/2/4292672/esea-gaming-network-bitcoin-botnet>> accessed March 9 2017

¹⁸⁸ www.reddit.com/r/GlobalOffensive/comments/36inncc/esea_client_update_questions_for_lpkane/

¹⁸⁹ *Ibid*

policy. The wording itself is basically sufficient in the sense that it makes clear that the anti-cheat software grants itself total and complete access to the user's terminal equipment. It is questionable, however, whether users are aware of the fact that ESEA runs in kernel mode and the implications thereof.¹⁹⁰ Interestingly, questions about the always-on nature of the software are apparently numerous enough to warrant filing under frequently asked questions. ESEA explains that it is always on because *'[m]uch like the leading anti-virus software, which are always running to prevent or detect viruses, the ESEA Client is running to prevent or detect cheats that may be running on a computer. This "Always On" feature is a necessary layer for the ever evolving cheaters we as a community face'*.¹⁹¹ In my view, this explanation comes dangerously close to misdirection because it purports a false equivalence to 'leading' anti-virus software (which operates to protect the user and is fully open as to what it does to the user's computer) and argues that the always-on feature is necessary, even though such functionality is highly unusual.¹⁹²

3.8 Conclusion

In conclusion, Article 5(3) of the ePrivacy Directive significantly restricts usage of client-side anti-cheat, particularly so when methods of detection cross the memory boundary inhibited by the game. Ultimately, the extent of the allowable intrusion depends heavily on the notion of informed consent. As asserted, both content and the way in which the information is conveyed are unlikely to meet the standard which client-side anti-cheat's intrusive character would demand. Commonly used, broad terms such as 'monitoring RAM' arguably cover basic techniques such as signature based detection and binary validation, but provide the user with too little information to justify the usage of techniques beyond that. With the direct restrictions to client-side anti-cheat explored, this thesis now turns its attention to restrictions of a more circumstantial nature.

¹⁹⁰ Kernel mode's complete access to the computer comes at a cost: if the anti-cheat software generates an error the consequence is a total system crash (resulting in the well-known 'blue screen of death'). With regards to the latter, see: <https://www.howtogeek.com/163452/everything-you-need-to-know-about-the-blue-screen-of-death/>

¹⁹¹ <https://play.esea.net/index.php?s=content&d=anticheat>

¹⁹² While I have no direct source for this, my own research into the various anti-cheat mechanisms (both third party and integrated) reveals that this functionality is unique to ESEA and not used anywhere else.

CHAPTER FOUR – THE RIGHT OF ACCESS TO PERSONAL DATA

4.1 Introduction

A related issue that warrants attention is the right of access to personal data under the GDPR. Data subjects have a right to access their personal data and other related information such as the purposes of the processing, the categories of personal data concerned, recipients, and so forth.¹⁹³ The right of access is a manifestation of the fair processing and transparency principles and aims to enable data subjects to verify the lawfulness of the processing.¹⁹⁴ The right to access is relevant because cheaters are rarely banned instantaneously but rather after a period of time following detection (in ‘waves’), or at least after manual review and verification.¹⁹⁵ One advantage to this approach is that you deny cheaters and cheat developers precious feedback with regards to what triggered the detection. However, this also means that some kind of record or file on confirmed or suspected cheaters is necessary. Access requests aimed towards such records or related information could be used to learn more about detection methods in use by the game company. Of course, whether such access requests demand consideration at all will depend on whether the information constitutes personal data.

4.2 Qualifying the cheating-dossier as personal data

In *Y.S. v Minister voor Immigratie*, the Court of Justice of the European Union found that a legal analysis as such is merely ‘*information about the assessment and application (...) of that law to the applicant’s situation*’ and did not ‘*relate to*’ the applicant.¹⁹⁶ It stands to reason that, in the same way, the records kept on suspected cheaters are (in part) a subjective account of an adherence to or violation of the rules. The information therein is – at least with regards to the analytical component – merely an ‘*assessment*’ or ‘*application*’ of technical and common sense knowledge to the player’s situation and therefore not personal data. The way in which the logic employed by the Court should be translated and applied to other situations is by no means self-

¹⁹³ Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ 281/31, art 12

¹⁹⁴ *Ibid*, Recital 41

¹⁹⁵ Nick Cano, *Game Hacking: Developing Autonomous Bots for Online Games* (No Starch Press 2016) 269

¹⁹⁶ Joined Cases C-141/12 and C-372/12 *Y.S. v. Minister voor Immigratie* [2014] ECLI:EU:C:2013:838 [40]

evident, however. Recital 63 of the GDPR, which deals with the right of access, states that ‘*[the right of access] includes the right for data subjects to have access to data concerning their health, for example the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided*’.¹⁹⁷ Applying the logic from *Y.S. v Minister voor Immigratie*, diagnoses or assessments would be mere applications of medical knowledge to the patient’s situation. While the assessment may *contain* personal data, the assessment as such would be considered an abstraction with no direct connection to the data subject by the Court – thus contradicting the terminology in Recital 63 of the GDPR. As a counter point to this position, one could argue that the legislator addresses a very specific situation here and that it is only for this situation that assessments would fall under the right of access (and thus constitute personal data). A medical analysis could be considered unique in the sense that personal data and the actual analysis itself are very likely to be intrinsically connected. However, it would be strange, to say the least, that the legislator would ‘casually’ mention assessments while enumerating a list of examples of personal data without explicitly mentioning that assessments are only held to be personal data in this one, particular instance.¹⁹⁸ This implies a level of oversight one cannot in good faith ascribe to the legislator, thus casting doubts on the generalizability of the findings of the Court. Moving on, the Court explicitly discerns between ‘*the factual basis of the legal analysis*’ and the legal analysis itself, of which the former may very well be personal data.¹⁹⁹ Even if we apply the logic of the Court to the case of online gaming, we will find that any

**Example
DNS-cache scanning**

1. *Raw materials:* websites the player visited (the player’s dns-cache).
2. *Analysis:* the blacklist to which these sites are compared.
3. *End-result:* binary conclusion as to whether the player visited blacklisted sites.

¹⁹⁷ Parliament and Council Regulation of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ 119/1, Recital 63

¹⁹⁸ Moreover, medical assessments and personal may be closely connected but they are not inseparable. In that sense they are no different from legal (as was at stake in *Y.S. v Minister voor Immigratie*) and technical (as is at stake in the case of anti-cheat) analyses: according to the Court’s approach, the medical professional would simply separate the personal data *contained* in the analysis (i.e. the patient’s characteristics) and disclose only that.

¹⁹⁹ Joined Cases C-141/12 and C-372/12 *Y.S. v. Minister voor Immigratie* [2014] ECLI:EU:C:2013:838 [45]

information detached from the analysis may still qualify as such. Take dns-cache scanning, for example. A list of websites visited by the data-subject is clearly *about* that person. Even if game companies apply proper safeguards and only hash-validate based on a blacklist, this merely flips the result: information concerning which websites a data subject *did not* visit is still personal data.²⁰⁰ In summary, even if *Y.S. v Minister voor Immigratie* is to be interpreted in such a way that analyses are excluded from being personal data, any raw materials (in so far they are kept on record)²⁰¹ and end-results will still qualify as such and are therefore subject to the right of access.

4.3 Limits to the right of access

There are limits to the right of access. Article 23 of the GDPR allows Member States to restrict rights of access and information if necessary in the interest of the data subject or to protect the rights and freedoms of others.²⁰² Moreover, Recital 41 of the Data Protection Directive states that *‘[the right of access] must not adversely affect trade secrets or intellectual property and in particular the copyright protecting the software; whereas these considerations must not, however, result in the data subject being refused all information’*.²⁰³²⁰⁴ The Trade Secret Directive, adopted on the 6th of June 2016, defines trade secrets as any information that is secret, has commercial value because it is secret, and has been subject to reasonable steps by the holder to keep it secret.²⁰⁵ Anti-cheat techniques have clear commercial value because they are secret: the holder of the trade secret will have a game less vulnerable to cheaters in comparison to other game companies. However, it is not always the methods themselves that require protection but

²⁰⁰ This follows from the traditional interpretation of personal data in the European Union (see: Article 4(1) of the GDPR). If the data is kept on record for the purpose of banning a particular player of account, the data subject is by definition identified. It relates to a person because it concerns the data subject’s activities. If, somehow, the raw materials for some particular technique are not clearly about a person (it is difficult whether to establish if this would ever be the case as the subject matter is very abstract and theoretical) the Article 29’s Working Party’s guidance on personal data suggests that any such information constitutes personal data regardless because it is kept on record 1. for the purpose of singling out the data subject, and 2. to cause an impact on the data subject’s interests. See: Article 29 Working Party, ‘Opinion 04/2012 on cookie consent exemption, WP194’ (2012) 9-12

²⁰¹ It stands to reason that, in most cases, game companies would destroy the raw materials as soon as possible to limit the privacy harm.

²⁰² Parliament and Council Regulation of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ 119/1, art 23

²⁰³ *Ibid*, Recital 63

²⁰⁴ These limitations are upheld in the GDPR.

²⁰⁵ Parliament and Council Directive 2016/943 of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure [2016] OJ 157/1, art 2

rather the information surrounding it.²⁰⁶ In this case, it is the detection *strategy* rather than detection methods as such that require protection. This situation is somewhat unusual because we tend to think of trade-secrets in the context of a company shielding its secrets from a direct competitor.²⁰⁷ Here, however, the game company primarily wants to keep its detection strategies as a whole hidden from their customers (cheaters) and indirect competitors (cheat developers), not other game companies.²⁰⁸ Unusual as the situation may be, there is nothing to suggest that detection strategies as a whole would not fit the definition in Article 2 of the Trade Secret Directive simply because its commercial value does not relate to direct competitors.

The Trade Secret Directive, however, ‘*respects the fundamental rights and observes the principles recognised in particular by the Charter, notably the right to respect for private and family life [and] the right to protection of personal data (...)*’.²⁰⁹ In order to balance the two rights, Malgieri proposes to decontextualize sensitive information. The idea is ‘*that customers can access only data strictly related to their biographical information while trade secret holders can be free not to disclose the output of their data processing (behavior evaluation, forecast, studies on life expectancy, personalized marketing plan, pricing, etc.) if disclosure can adversely affect their interests*’.²¹⁰ His proposed solution of data de-contextualization is, at least for the case of online gaming, problematic. This approach merely circumvents the problem rather than solving it: any personal data which has the potential to reveal sensitive information concerning trade secrets is simply erased from the equation.²¹¹ Moreover, the problem when applying this method to the case of online gaming is that cheat developers are potentially able to use *any*

²⁰⁶ Valve’s use of dns-cache analysis, for example, was a novel and innovative way of catching cheaters and would almost certainly meet the definition. However, at some point later in time, after the method itself became publically known, another game company or even Valve itself may choose to re-deploy it.

²⁰⁷ See, for example: Director Magazine, ‘Trade Secrets of Business’ (Director.co.uk, May 8 2016)

<<http://www.director.co.uk/news-trade-secrets-17924-2/>> accessed March 9 2017

²⁰⁸ Other game companies would learn nothing that would allow them to compete more effectively with one another. Only knowledge that relates to specific detection methods as such would allow them to add to their own arsenal. Knowledge of well-understood techniques being used by other game companies benefits them in no way, as they are not in direct competition with one another (at least on this front).

²⁰⁹ Parliament and Council Directive 2016/943 of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure [2016] OJ 157/1, Recital 34

²¹⁰ Gianclaudio Malgieri, ‘Trade Secrets v. Personal Data: a possible solution for balancing rights’ [2016] 6(2) International Data Privacy Law 102, 102

²¹¹ It also fails to recognize that personal data is so much more than only biographical information.

information with the slightest relation to anti-cheat functionality to their benefit.²¹² For example, the mere knowledge that a screenshot has been taken of my computer (without even having to know its contents) may aid me in determining how anti-cheat functionality is being executed. Taking all of the above into account, it stands to reason that trade secret holders will be intrinsically motivated to disclose as little personal data as possible, possibly to the point of it being unlawful. Game companies are (understandably) biased towards their own interests and it is questionable whether they can objectively assess when personal data is sufficiently far removed from sensitive information in order to be disclosed. It is not surprising that the European Data Protection Supervisor has proposed that national data protection authorities should become involved every time rights of access and trade secrets conflict.²¹³ An interesting idea to be sure, but cheat detection's niche character would require a significant degree of technical knowledge which national data protection authorities simply do not possess. Data protection authorities are also notoriously understaffed, casting further doubt on the feasibility of this proposal.²¹⁴

Malgieri, from the perspective of a literal interpretation of the available legal text, comes to the conclusion of a '*legislative favor for data protection rights*' despite ascertaining the presence of a non-prevalence rule.²¹⁵ Because the literal rule suffers from significant limitations and has often been criticized as '*fundamentally defective*'²¹⁶ due to language being inherently imprecise²¹⁷ and the possibility of unintended absurdities,²¹⁸²¹⁹ this approach holds little value. Assessing the case of online gaming and anti-cheat on its own merits is therefore required. Alexy, in his work on constitutional rights, has introduced a 'law of balancing': '*the greater the degree*

²¹² Worded differently, it is impossible to know how much a potential cheat developer already knows through reverse engineering, and what further information he needs to verify or otherwise supplement that which he has already learned.

²¹³ Gianclaudio Malgieri, 'Trade Secrets v. Personal Data: a possible solution for balancing rights' [2016] 6(2) International Data Privacy Law 102, 105

²¹⁴ Annemarie Spokkereef and Paul de Hert, 'Biometrics, Privacy and Agency' in Emilio Mordini and Dimitros Tzovaras (eds) Second Generation Biometrics: The Ethical, Legal and Social Context (Springer 2012) 87 International Data Privacy Law 102, 104-105

²¹⁶ Ian McLeod, *Legal Method* (Third Edition, MacMillan Press Ltd., 1999) p. 253

²¹⁷ DPP v. Ottewell [1970] AC 642,649 (Cr. App)

²¹⁸ Ian McLeod, *Legal Method* (Third Edition, MacMillan Press Ltd., 1999) p. 253

²¹⁹ Credit to the following article for pointing towards the sources in footnotes 215 and 216: LawTeacher, 'Advantages And Disadvantages Of The Literal Rule Constitutional Law Essay' [2013] *Lawteacher.net* <<https://www.lawteacher.net/free-law-essays/constitutional-law/advantages-and-disadvantages-of-the-literal-rule-constitutional-law-essay.php#ftn25>>

of non-satisfaction of, or detriment to, one principle, the greater must be the importance of satisfying the other'.²²⁰ In line with this approach, establishing whether excluding the cheating-dossier from the right of access is justified means determining the following: 1. the degree of detriment to the principle of transparency (right of access), 2. the degree of satisfaction of the principles of '*economic freedom and freedom of the intellectual property of the business*',²²¹ (trade secrets), and 3. '*whether the importance of satisfying the latter principle justifies the detriment to the former*'.²²²

The detriment to the principle of transparency is limited. Some data subjects may want to verify the accuracy of the personal data kept on record, but information which reflects poorly on the data subject (in the sense that it reveals them as a cheater) is likely to be disputed, regardless of whether it is accurate or not. The right of access's value is, in this respect, questionable. Verifying the lawfulness of the processing would be equally problematic due to the fact that most disputes over lawfulness will likely center around the point of origin, i.e. whether the initial access under Article 5(3) was lawful. The problem is that data subjects would need detailed access to game companies' anti-cheat techniques to be able to determine lawfulness.²²³ They would also need a high degree of technical proficiency, incidentally something only those with a background in cheat-development or reverse engineering (in other words, exactly those who are likely to use the right of access maliciously) are likely to possess. Finally, it stands to reason that personal data pertaining to cheating constitutes only a small part of the personal data on record.²²⁴ On the other hand, forcing game companies to disclose personal data from records pertaining to cheaters would greatly hurt their ability to keep the game (sufficiently) cheat-free and cut into profits. This will cause a chilling effect on future online game development and undermine the market as a whole. In the extension of this, consumers also have a clear interest and should not be disregarded: they pay for online games and accordingly expect a product of a

²²⁰ Sybe de Vries, 'Balancing Fundamental Rights with Economic Freedoms According to the European Court of Justice' (2013) 9(1) Utrecht Law Review 169, 170

²²¹ Gianclaudio Malgieri, 'Trade Secrets v. Personal Data: a possible solution for balancing rights' [2016] 6(2) International Data Privacy Law 102, 115

²²² Sybe de Vries, 'Balancing Fundamental Rights with Economic Freedoms According to the European Court of Justice' (2013) 9(1) Utrecht Law Review 169, 170

²²³ In other words, whereas access to the cheating dossier may indirectly reveal sensitive information concerning detection methods, verifying lawfulness would require directly revealing the technical specifics of such methods, thus practically ensuring that trade secrets will become compromised.

²²⁴ In other words, the right of access can still be invoked for most of the total record.

certain quality and games infested with cheaters are unlikely to meet this expectation. From a utilitarian perspective, the interests of a very large group of consumers outweigh the interests of the lone data subject who on rare occasion will in good faith file an access request.²²⁵ Taking all of the above into account, the importance of satisfying the economic freedom and freedom of intellectual property rights of game companies outweighs the detriment to the principle of transparency. Allowing companies to restrict the right of access as they see fit to protect trade secrets (within reason) is therefore justifiable. To compensate, game companies should inform users of this restriction via the terms and conditions prior to asking consent. One other significant way in which this discrepancy can be compensated – thus further justifying the choice for this particular balance – will be discussed in chapter five.

4.4 Conclusion

In conclusion, the right of access to personal data and trade secrets are at significant odds with one another. While, depending on interpretation, the analysis itself may or may not qualify as personal data, the raw materials and end-result certainly will. Following a pragmatic approach, this thesis came to a balance in favor of trade secrets. While I have criticized Malgieri's approach of data de-contextualization, my own analysis ironically arrives at the same end-result: data protection rights take a back-seat to businesses' trade secrets. Chapter five will now revisit the issues enumerated in chapter three, and assess to what extent a similar balance can or should be struck.

²²⁵ I am of course aware that these consumers and data subjects are the exact same group. Yet, the amount of people in that group expecting a quality product will vastly outnumber the amount of people would actually file an access request in good faith.

CHAPTER FIVE – RE-CONCEPTUALIZING INFORMED CONSENT

5.1 Introduction

The two key issues discussed in chapter three and four – informed consent and the right of access to personal data – are in fact two different manifestations of the same problem: a tension between the right to trade secrets on the one hand and a right to information on the other.²²⁶ In order to gain a full understanding of the way in which the ePrivacy Directive restricts usage of client-side anti-cheat, it must be determined whether – similarly to the right of access – the notion of informed consent can be restricted in order to safeguard trade secrets.

5.2 Informed consent versus trade secrets

The ePrivacy Directive does not recognize any other exception to the requirement of consent to access a user’s terminal equipment aside from those already mentioned in Article 5(3). Article 11 of the ePrivacy Regulation proposal does allow for Union or Member State law to restrict the scope of the obligations and rights provided for in Articles 5 to 8 by way of legislative measure in order to safeguard public interests referred to in Article 23 of the GDPR. However, trade secrets would fall under 23(i): ‘the rights and freedoms of others’ and Article 11 of the ePrivacy Regulation Proposal does not allow for this particular provision to be restricted. As such, it appears as if there is no legal basis through which consent’s informational component can be restricted in order to preserve trade secrets. The literature unfortunately offers no guidance either: whereas scholarly debate concerning the conflict between trade secrets and the right of access was scarce, debate concerning the conflict between trade secrets and informed consent is absent altogether. Interestingly, Article 4 of the ePrivacy Directive, which requires electronic communications service providers to ensure the security of their networks, suffers from a similar problem: electronic communications service providers may be faced with the paradoxical obligation to inform data subjects under investigation for threatening the security of the network of the fact that they are being investigated. Here, also, no scholarly debate or legal literature exists from which to draw. It appears as if the right to information has been explored and developed in isolation rather than in aggregate. On the one hand, this poses problems as there is

²²⁶ There is of course no ‘right of information’ as such, I am instead referring to the right of access to personal data and the right to being provided with information prior to consenting in aggregate.

little to no prior theory and analysis from which to draw. On the other hand, the lack of set-in-stone beliefs and firmly established doctrines allow for an open-minded perspective which may give rise to new and creative solutions. Having determined that neither the law itself nor the literature provides any guidance on how this conflict should be resolved, this thesis now turns its attention to proposing a new solution altogether.

5.3 Substantiating informed consent for the case of online gaming

Prior to any remedy being necessary, there are several steps which game companies can reasonably take in order to address some of the shortcomings addressed in chapter three without having to expose information related to trade secrets. Most notably, game companies should follow Blizzard's Entertainment's example of a separate anti-cheat agreement because this makes the information significantly more visible at virtually no cost to the game company. It can be said with reasonable certainty that the average user is unlikely to be familiar with or aware of client-side anti-cheat and its consequences. If the anti-cheat provisions are hidden in the privacy policy or terms of service then, realistically, only a very small subset of users would become aware of them. Consent fatigue – the phenomenon where users are required to agree to terms so often they just blindly agree to them – is well documented.²²⁷ Despite the fact that game companies can never be sure users actually read terms, separate anti-cheat agreements would at least grant the user a fair opportunity to do so. With regards to the content of the terms, terms should clearly signify that the right of access to personal data is restricted and that the content of the terms may be incomplete due to secrecy reasons. Terms should also make clear whether the anti-cheat crosses the memory boundary inhibited by the game and whether it runs in kernel mode.²²⁸

5.4 Making the case for informed consent

Some readers may wonder, after being confronted with the quagmire that is informed consent,

²²⁷ European Commission, 'Ex-Post REFIT evaluation of the ePrivacy Directive 2002/58/EC' (Commission Staff Working Document, 2017) 42

²²⁸ One could argue that this information is part of the anti-cheat strategy as a whole and is therefore protected as a trade secret. However, this argument is not convincing because these things are relatively easily discovered via a quick Google search or minor effort in reverse engineering and therefore do not meet the trade secret definition posed by Article 2(1) of the Trade Secret Directive. Both components must therefore be included in the provision of information.

can consent ever truly be informed? And even if we do somehow have all the facts and fully understand them, does that mean that consent is necessarily rational? The idea of informed consent can be traced back to the notion of autonomy and the belief that individuals should be able to shape their own destiny.²²⁹ The idea has however been criticized due to emotion²³⁰, logical fallacies²³¹, and other limitations such as memory impeding the decision making process: even in the face of perfect knowledge, decisions are unlikely to be purely rational. Taking this argument to the extreme, if we are essentially unable to take rational decisions on the basis of prior information, then the notion of ‘informed consent’ is legal fiction. This problem has garnered significant attention, particularly in the area of bio-ethics. Meisel remarks that the notion of informed consent ‘*has often been condemned by the medical community as a myth (...)* [but] *has been generally praised by legal scholars*’.²³² At the same time, it is recognized that informed consent may be morally compelled.²³³ The ‘*duty*’ of informed consent ‘*is a reflection of wider cultural values about the moral importance of respect for individual autonomy*’.²³⁴ It is of course possible to criticize the case for informed consent by arguing that it is pointless to impose a moral obligation which can never be fulfilled.²³⁵ And if we cannot make truly informed and rational decisions, how can we willingly part with the fundamental right to bodily integrity, privacy, or any other? These criticisms have merit but are mostly academic in nature. Rejecting the idea of informed consent altogether would lead to a total breakdown of day to day life. Even though informed consent does not necessarily equal rational consent, its symbolic power is indisputable: it fulfills our inherent desire to inform ourselves and make our own decisions about important matters in life. Who among us would be comfortable with our doctors planning medical procedures for us because our own decisions are not guaranteed to be entirely rational?

²²⁹ Berg and others, *Informed Consent: Legal Theory and Clinical Practice* (2nd edition, Oxford University Press 2001)

²³⁰ See, for example: Norbert Schwarz, ‘Emotion, cognition and decision making’ [2004] 14(4) *Cognition and Emotion* 433

²³¹ See, for example: Michael LaBossiere, ‘Forty Two Fallacies’ (2002) <<https://aphilosopher.files.wordpress.com/2010/09/42-fallacies.pdf>> accessed 14 May 2017

²³² Alan Meisel, ‘The Exceptions to the Informed Consent Doctrine: Striking a Balance Between Competing Values in Medical Decision Making’ [1979] 2 *Wisconsin Law Review* 413, 413

²³³ See, for example: Mark Sheehan, ‘Can Broad Consent be Informed Consent?’ (2011) 4(3) *Public Health Ethics* 226; Satyanarayana Rao, ‘Informed Consent: An Ethical Obligation or Legal Compulsion?’ (2008) 1(1) *Journal of Cutaneous and Aesthetic Surgery* 33

²³⁴ Len Doyal, ‘Informed Consent: moral necessity or illusion?’ (2001) 10(1) *Quality in Healthcare* 29, 29

²³⁵ Paraphrased from: *Ibid*, 30

And who would go a step further and extend such trust to large corporations, who, unlike doctors, are not bound by ethical codes and strict professional guidelines? The value of criticizing informed consent, then, lies not in providing a justification for abandoning it but instead in the fact that it helps in exposing, acknowledging and addressing its limitations. Taking all of the above into account, I argue that Article 5(3)'s sole reliance on consent is justified and must be maintained by way of moral obligation. Just like the surgeon's scalpel, devices that enter the user's terminal equipment are invasive and infringe upon spaces explicitly protected by fundamental human rights. While the harms and risks are different and quite arguably not as serious, I consider them serious enough to afford consent the same key role. And I am certainly not alone in that conviction: ninety-two percent of respondents to the Eurobarometer survey considered it important their permission be asked before being subjected to tools that monitor their activities online.²³⁶ The question whether we can ever be truly informed or make truly rational decisions is philosophically interesting, but does not in itself constitute a convincing argument in favor of abandoning informed consent. Doing so would mean giving up a hard-fought '*right of individuals to exercise control over [an aspect] of their lives that they deem critical*'. Finally, the European Commission also considers the role of Article 5(3) to be to '*empower users vis-à-vis their private sphere, giving them the possibility to decide over the content and access to their device*', implying that consent's key role should indeed be maintained.²³⁷ In summary, although authors with different views on concepts such as autonomy and the value of informed consent may arrive at a different conclusion, I personally support the more indeterministic worldview that informed consent – despite all its flaws – indeed allows us to shape our own destinies and should absolutely be pursued.

Some have proposed incorporating 6(f) of the GDPR – the legitimate interest – into the ePrivacy Regulation as a lawful ground for access.²³⁸ Aside from the substantial detriment to autonomy this would cause (as asserted above), transparency would also be impacted; it would lead to a situation where controllers are under no obligation to disclose *any* information prior to

²³⁶ European Commission, 'Ex-Post REFIT evaluation of the ePrivacy Directive 2002/58/EC' (Commission Staff Working Document, 2017) 40

²³⁷ *Ibid.*, 46

²³⁸ See, for example: IAB Europe, 'Position on the Proposal for an ePrivacy Regulation' (2017) <http://iabireland.ie/wp-content/uploads/2017/03/20170328-IABEU-ePR_Position_Paper.pdf> accessed 7 March 2017

access or storage as long as no personal data is collected.²³⁹ Consent is valuable because it acts as a gatekeeper by guaranteeing that the user is supplied with the necessary information in a clear and visible way, as it can only be valid when it meets these standards. As discussed in chapter four, this thesis departs from the idea that satisfying game companies' economic freedom and freedom to intellectual property in the context of anti-cheat is important and should indeed be satisfied. Invoking once again Alexy's law of balancing, the question then becomes how we can limit the detriment to transparency and autonomy as much as possible to the point where satisfaction of game companies' economic freedom and right to intellectual property can be considered justifiable.²⁴⁰ In line with this approach, the benchmark must be to ensure, to the greatest extent possible, that users have '*full information of all relevant issues*'.²⁴¹

5.5 Informed consent by way of third party

In bio-ethics, it has been recognized that a more paternalistic approach to patient consent may be appropriate.²⁴² While some authors believe patients should always make their own decisions, the idea of the '*isolated, perfectly rational, prudential decision maker*' is fiction.²⁴³ Many patients even actively choose to delegate or share decision making with others. Drawing inspiration from these ideas, my proposal is to bridge the 'information gap'²⁴⁴ by introducing a trusted third party into the equation. This third party will not only have all the facts at their disposal but will also possess the necessary knowledge and expertise to properly interpret those facts and convey them to the data subject. Naturally, the third party will be subject to strong confidentiality obligations in order to ensure that game companies' trade secrets stay secret. This proposal may appear somewhat hypocritical at first. After all, I have previously argued that Article 5(3)'s sole reliance on consent is morally compelled, but now propose to alter it in a way which would seemingly

²³⁹ This is due to the fact that the ePrivacy Regulation in itself does not stipulate any specific information requirements (separate from consent) like the GDPR does.

²⁴⁰ Some kind of value judgment is, of course, inevitable. The smaller the detriment to the principles of transparency and autonomy, the more justifiable the solution of excluding certain types of personal data becomes.

²⁴¹ Article 29 Working Party, 'Opinion 4/2007 on the definition of consent, WP187' (2011) 19

²⁴² See, for example: Mark Sheehan, 'Can Broad Consent be Informed Consent?' (2011) 4(3) *Public Health Ethics*; Emma C Bullock, 'Informed Consent and Justified Hard Paternalism' (PHD Thesis, University of Birmingham 2012)

²⁴³ Gail Van Norman, 'Informed Consent: Respecting Patient Autonomy' in Van Norman and others (eds) *Clinical Ethics in Anesthesiology: A Case-Based Textbook* (Cambridge University Press 2011) 36

²⁴⁴ Meaning, the (lack of) information as game companies provide it, and the information that they should be providing in order for consent to be considered informed.

diminish its role. The intent here, however, is not to take the decision out of the user's hands, but rather to rephrase the necessary information in a way which is fair to both parties. In doing so, the user gains '*an appreciation and understanding of the facts and implications*' of consenting, without having to know in full detail the precise specifications of detection methods or possess the necessary technical expertise to make sense of it.²⁴⁵ Implemented and executed properly, this proposal keeps the system of informed consent intact while at the same enabling game companies to keep their anti-cheat strategies concealed. It is clear a system like this can only work if the trustworthiness of the third party is guaranteed. Certification should be used to achieve this. Certification and privacy seals have long since been discussed²⁴⁶ but have now been incorporated in the GDPR²⁴⁷ '*in order to enhance transparency and compliance [with the regulation]*'.²⁴⁸ They allow '*data subjects to quickly assess the level of data protection of relevant products and services*'²⁴⁹ and have been hailed as a possible solution to the problem that users generally do not read standardized terms or do not comprehend them due to legal jargon, which makes it particularly well suited to the problem at hand.²⁵⁰ Because the benchmark is to ensure that users have – to the greatest extent possible – '*full information of all relevant issues*'²⁵¹ – the certifying body should first and foremost:

1. Review the detection strategy as a whole and grade it on a scale from not invasive at all to highly invasive. The level of invasiveness determines the type of privacy seal granted (of which there would be several) which should be displayed in the anti-cheat agreement. A link should be provided to the website of the certifying body, where each level of invasiveness is explained in more detail and by using examples. This will aid the user in making a decision which is not only informed, but also as rational as possible.

²⁴⁵ Article 29 Working Party, 'Opinion 4/2007 on the definition of consent, WP187' (2011) 19

²⁴⁶ Rowena Rodrigues, David Wright and Kush Wadhwa, 'Developing a privacy seal scheme (that works)' (2013) 3(2) International Data Privacy Law 100, 100

²⁴⁷ Parliament and Council Regulation of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ 119/1, art 42

²⁴⁸ *Ibid*, Recital 100

²⁴⁹ *Ibid*

²⁵⁰ Rodrigues and others, 'The future of privacy certification in Europe: an exploration of options under article 42 of the GDPR' 30(3) International Review of Law, Computers & Technology 248, 249

²⁵¹ Article 29 Working Party, 'Opinion 4/2007 on the definition of consent, WP187' (2011) 19

However, users cannot reasonably put their trust into a certification system without a last line of defense to protect against situations where they risk consenting to something no reasonable, informed and rational person would have consented to. As such, the certifying body should also:

2. Assess whether any of the techniques in use are so invasive that they are either: 1. out of line with the reasonable expectations of an average, reasonable user; or 2. otherwise unlawful. An example of the former would be ESEA's always-on functionality.²⁵² A hypothetical example of the latter would be a technique which is designed to come into contact with personal data (via window titles, for example) but systematically neglects to minimize the privacy intrusion by way of (for example) hashing and pseudonymization techniques.²⁵³²⁵⁴

Finally, in order to further justify the decision to let the right to trade secrets prevail over the right to information (as asserted in chapter 4), the certifying body should play an active role in alleviating that discrepancy. The main purpose of the right of access is to enable data subjects to verify the lawfulness of processing of their personal data.²⁵⁵ Therefore, the certifying body should also:

3. On request, verify the lawfulness of the processing concerning any data which is withheld by the game company due to secrecy reasons. In case of a complaint, the certifying body will take an active role and use its knowledge and expertise to determine whether the personal data withheld indeed shares a significant enough connection to trade secrets.²⁵⁶

Implementing this system will require changes to the legislature. Article 9 of the ePrivacy Regulation proposal should be amended with a provision such as the following:

²⁵² It is conceivable that this functionality would fall within the user's reasonable range of expectation if ESEA would call clear attention to it and be as transparent as possible in the terms and conditions.

²⁵³ The justification for this lawfulness-test (which, after all, other controllers in different areas of business are not subjected to) lies in the fact that users are left in the dark as to the specifics of anti-cheat and are completely unable to gauge lawfulness for themselves and hold the controller accountable as a result.

²⁵⁴ The other side of the coin is that companies which make a point to implement such techniques and minimize the privacy harm wherever possible would be rewarded because their anti-cheat strategy can be considered less invasive as a result.

²⁵⁵ Parliament and Council Regulation of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ 119/1, Recital 63

²⁵⁶ While not as far-reaching as the European Data Protection Supervisor's proposal to involve an official entity in each case where the right of access and trade secrets conflict, this proposal achieves a similar effect.

*In so far restricting the provision of information is necessary in order to preserve trade secrets, certification shall be used as a compensatory measure to ensure that access to end-users' terminal equipment is lawful, and in line with the reasonable expectations of data subjects based on the terms provided.*²⁵⁷

Rather than allowing several certifying bodies to exist in competition with one another, only one certifying body should be established. This fits the European Commission's belief that the number of privacy seal systems should be kept to a minimum.²⁵⁸ The certifying entity should be a separate EU body closely connected to the European Data Protection Board (or an appointed Data Protection Authority).²⁵⁹ Structuring the system in this manner addresses several common criticisms against privacy seals, such as a lack of regulatory oversight (one single entity closely connected to the European Data Protection Board allows for effective oversight) and forum shopping by companies (once again, there is only one entity to choose from). Lack of harmonized standards will also not be a problem as only one set will exist. In order to be able to carry out the assessment, the certifying body should consist of experts specialized in privacy, data protection, game design and anti-cheat. Due to the sensitivity of the information, experts carrying out the assessment will need to sign strong confidentiality agreements.

Ideally, game companies should seek certification prior to deploying new methods of detection. This will encourage them to employ value-sensitive design and ensure that privacy considerations are taken into account from the start of the development process. This will cause a shift in focus from purely technological considerations (i.e. how well is the system going to perform) to legal and ethical considerations (i.e. how well will the system perform while simultaneously minimizing the privacy harm). That shift in thinking will require additional resources and, while hampering innovation from a purely technological perspective, will simultaneously stimulate a different type of innovation which is not measured purely in

²⁵⁷ The first part of this provision is self-explanatory. With regards to the second part, '*based on the terms provided*' accounts for the fact that game companies have influence over what constitutes a reasonable expectation. For example, if a company clearly signifies that highly invasive methods are used in the terms and conditions (and makes this information sufficiently visible) the threshold as to what users should reasonably expect changes. NB: Substantive requirements for certification itself should be set out in another, separate provision.

²⁵⁸ Rowena Rodrigues, David Wright and Kush Wadhwa, 'Developing a privacy seal scheme (that works)' (2013) 3(2) International Data Privacy Law 100, 104

²⁵⁹ Practically speaking, there are only a limited amount online games with integrated anti-cheat and third party anti-cheat software applications currently out or coming out in the future. I predict that, aside from the initial hurdle of certifying all the online games already released, this would not be an unrealistic endeavor.

technological prowess but rather in its ability to be technologically effective while at the same time respecting privacy.²⁶⁰ Finally, this proposal also has the added benefit of what Morgan and Yeung describe as regulation through communication.²⁶¹ By communicating levels of invasiveness to (would-be) customers, companies are indirectly encouraged to strive for an anti-cheat strategy which is as non-invasive as possible (as the hypothesis is that customers are more likely to choose such a product or service,)²⁶², thereby limiting the privacy harm. The risk of being perceived as a company which does not respect its users' privacy has been aptly described by Gabe Newell, CEO of Valve: *'There is also a social engineering side to cheating, which is to attack people's trust in the system. If "Valve is evil - look they are tracking all of the websites you visit" is an idea that gets traction, then that is to the benefit of cheaters and cheat creators. VAC is inherently a scary looking piece of software, because it is trying to be obscure, it is going after code that is trying to attack it, and it is sneaky. For most cheat developers, social engineering might be a cheaper way to attack the system than continuing the code arms race (...).'*²⁶³ Indeed, it should be noted that such a system need not only be a burden or restriction to companies. The other side of the coin is that being awarded certification will be beneficial in addressing already existing issues concerning trust and protect game companies against attacks on their reputation via social engineering.

Several further objections to this idea can be raised. First of all, certification under the GDPR is supposed to be a voluntary process by which controllers and processors can demonstrate compliance. In addition, with only one certifying body to choose from, it is becoming clear that – while beneficial to users – the impact on businesses' autonomy should also be considered. With the only options being risking fines, exposing trade secrets, abandoning client-side anti-cheat or seeking certification, the incentive to seek the latter is so strong that it becomes questionable whether certification can be considered truly voluntary. This is true, but the reality is that game companies already find themselves in an advantageous position over users, who are required to consent to an elaborate contract drafted by them from a take-it or leave-it position. Mitigating the disparity and thus improving autonomy for one party may come

²⁶⁰ What may follow, for example, is an increased focus on innovating server-side anti-cheat, which is less invasive.

²⁶¹ Bronwen Morgan and Karen Yeung, *An Introduction to Law and Regulation* (Cambridge University Press 2007) 96-102

²⁶² This process could also be characterized as and related to the market as a modality of regulation, see: Lawrence Lessig, *Code and other laws of cyber space* (Basic Books 2006) 123

²⁶³ Quoted from: https://www.reddit.com/r/gaming/comments/1y70ej/valve_vac_and_trust/

at the expense of the other.²⁶⁴ Moreover, it is the game company who is legally at fault when they employ detection methods without disclosing them, not the user. Certification is an opportunity to continue reaping the benefits of these devices while being in accordance with the law. Claiming damage to businesses' autonomy because they cannot continue profiting from an unlawful situation is therefore not a convincing argument.²⁶⁵ Second of all, certification is inherently problematic exactly because '*questions of trust and confidence are pushed back from the certified entity to the certifying body*'.²⁶⁶ Anti-cheat's niche character means that the pool of knowledge and expertise required to carry out the duties enumerated prior will most likely require attracting experts with prior experience in those fields. However, there is a real risk of partisanship as these experts are likely to have a history as cheat developers, reverse engineers or cheat analysts from the online gaming industry. Strong confidentiality agreements and screenings prior to hiring will be key here. The assessment procedure itself should be structured in such a way as to de-contextualize the information based on which the experts carry out their assessments. This could mean, for example, that experts perform their assessments without knowing exactly which company it concerns. Third of all, feasibility is also a valid concern. Limiting the amount of certification bodies to one has distinct advantages but raises questions as to whether this is realistic when considering workload. Although there are no exact estimates to how many online gaming companies employ client-side anti-cheat, my own research suggests that the amount of notable²⁶⁷ online games catering to European audiences and employing client-side anti-cheat is manageable. Moreover, not every company will choose to seek certification. The initial hurdle of certifying all these existing online games admittedly take time, but this is inevitable and not in itself problematic. Games with the largest amounts of players should be prioritized (as to guarantee the greatest possible benefit to the largest amount of users in the

²⁶⁴ To further ensure a fair balance where both parties benefit, the ePrivacy Regulation should also be amended with an article similar to article 83(2)(j) of the General Data Protection Regulation, which stipulates that adherence to approved certification mechanisms shall be duly considered when imposing fines.

²⁶⁵ Lastly, it should be noted that certification as a concept need not necessarily be voluntary and the idea of mandatory certification is not unheard of. For example, research commissioned by the European Commission has considered the possibility of introducing mandatory certification for user generated content providers in order to counter the problems with information provision via privacy policies. See: European Commission, 'Consumer Sentiment Regarding Privacy on User Generated Content Services in the Digital Economy (Consent)' (European Policy Brief 2013) 8

²⁶⁶ Paraphrased from: Rodrigues and others, 'The future of privacy certification in Europe: an exploration of options under article 42 of the GDPR' 30(3) *International Review of Law, Computers & Technology* 248, 249

²⁶⁷ Meaning, with significant amounts of players.

shortest possible time-frame). Game companies who have filed a request should be permitted to continue their current anti-cheat strategies (within reason) in order to account for the delay and facilitate a transition period. Clear instructions as to which information needs to be provided should be made available in advance in order to speed the process along. One of the technical experts interviewed for the purpose of this thesis confirms the feasibility of the proposal and raises several comments of worth. He concurs with the idea that pre-determined procedures and informational requirements would greatly speed up the process. In his view, development of a proprietary set of tools for the certifying entity to aid in the analysis of client-side methods could speed it up further.²⁶⁸ The most important variable is the competency of the developers: *‘If the game company has competent developers that know their system inside-out and can convince the security firm that they know what they're doing, then the audit is completed very quickly. If no one knows what they're doing, then honestly the sky's the limit.’*²⁶⁹ Generally speaking, however, he estimates a process like this to take around a month per game company, with the potential of several assessments being carried out simultaneously.²⁷⁰ Finally, someone will have to bear the costs of certification. Because game companies are the ones who benefit from continued usage of client-side anti-cheat devices, they are the most logical choice in this regard.²⁷¹ Moreover, this has the added benefit of further encouraging shifts in development towards privacy-friendly alternatives. When companies are thinking about an invasive anti-cheat strategy, the question becomes ‘why’ rather than ‘why not’.²⁷²

²⁶⁸ See: Annex C(2)

²⁶⁹ *Ibid*

²⁷⁰ The total length of the assessment will depend on in how much detail compliance to the law will be ascertained. Seeing as how the main objective is to convey a general level of invasiveness and determining whether the user consents to something unreasonable or *clearly* unlawful, the level of detail to be pursued is debatable. For example, should every statement made by the game company be technologically verified or do we assume accuracy in good faith? I have refrained from making definitive statements as to how deep that level of detail should be because these types of questions are not well-suited to a first draft of a (still mostly theoretical) proposal.

²⁷¹ They can also choose as to whether to delegate the costs to users.

²⁷² As such, costs should also be proportional to the length of the assessment. This will also encourage companies to be cooperative and speed along the process, while simultaneously being fair to smaller companies (who’s anti-cheat strategies will generally be smaller and less intricate, and therefore take up less time in assessment).

5.6 Conclusion

In closing, a single certifying entity which 1. assesses and conveys to the user the general level of invasiveness of the anti-cheat strategy, 2. verifies whether the anti-cheat strategy lies within reasonable expectation or is clearly unlawful, and 3. allows users to exercise the right of access by proxy, would lead to an only small detriment to transparency and autonomy for the user (and will in a certain way even be a boon, as the information is more visible via a privacy seal and easier to understand for non-experts) while simultaneously preserving trade secrets. Considering the importance of the benefit which is achieved, namely satisfying game companies' economic freedom and right to intellectual property, this proposal holds significant promise in being able to resolve the tension between the interests at stake in a way which is fair to all parties involved. While implementing this system would not be without obstacles (such as, for example, cost and ensuring the trustworthiness of experts), all of those obstacles can be overcome with sufficient care and planning.

CHAPTER SIX – CONCLUSION

6.1 Answering the research question

Client-side anti-cheat raises legal concerns from a privacy and data protection perspective because it intrudes upon users’ devices – which are explicitly considered to be part of the private sphere in line with the ePrivacy Directive (and upcoming ePrivacy Regulation). In the past, many have claimed (certain types of) client-side anti-cheat to be unlawful, but – upon closer inspection – do not provide the necessary evidence to substantiate that claim. In academia, the relationship between client-side anti-cheat and the European Union privacy and data protection legal framework has remained essentially unexplored which severely complicates verifying or disputing claims such as the one above. With online gaming becoming more and more popular, the matter can no longer be ignored. Consequently, this thesis set out to answer the following research question:

How do the ePrivacy Directive and GDPR restrict or otherwise limit usage of client-side anti-cheat by online gaming companies?

The ePrivacy Directive restricts usage of client-side anti-cheat through Article 5(3) by requiring consent for usage of any techniques marked in red. Techniques marked in green do not require consent (and are therefore considered ‘unrestricted’) because they fit the ‘strictly necessary’²⁷³ exception that Article 5(3) provides.

Technique	ePrivacy Directive (‘strictly necessary’)	ePrivacy Regulation proposal (‘necessary’)
Binary validation (constrained) ²⁷⁴	Green: unrestricted by Article 5(3): no consent or provision of information required	
Signature based detection (constrained)	Depends on whether ‘game code’ constitutes personal data	

²⁷³ Or the ‘necessary’ exception under the ePrivacy Regulation proposal.

²⁷⁴ Limited to the memory space inhibited by the game.

	or not ²⁷⁵	
Binary validation (unconstrained) ²⁷⁶	Red: restricted by Article 5(3).	
Signature based detection (unconstrained)		
Screenshots		
DNS-cache scanning		
Enumerating active processes and window titles		
Engaging kernel-mode		

As discussed throughout chapter two and three, many more techniques are bound to be in use but cannot be investigated as they are kept secret. As a rule of thumb, however, any technique which crosses the memory boundary inhibited by the game is very likely to require consent from the user. This is a logical consequence of the underlying rationale of Article 5(3), which holds the user’s terminal equipment – just like his or her domicile – to be part of the private sphere. The *extent* of the restriction, then, depends on the way in which we interpret the requirements for valid consent in the online gaming context. The ePrivacy Directive and ePrivacy Regulation proposal define consent by referring to the DPD and GDPR respectively. And this is where things begin to get murky. As I have argued in chapter three, the legislator’s decision to ‘import’ consent’s requirements in this way is a mistake because consent under the GDPR deals with an entirely different situation. While it is true that information collected from the user’s terminal equipment may constitute personal data, Article 5(3) is first and foremost a privacy protection mechanism: it protects against unauthorized access to users’ terminal equipment regardless of whether the information therein constitutes personal data. And exactly *because* it deals with a fundamentally different situation, fundamentally different kinds of information may be required to consider users adequately informed. The ePrivacy Directive therefore leaves us without any

²⁷⁵ See: paragraph 3.5 and 6.2.

²⁷⁶ Not limited to the memory space inhibited by the game.

guidance as to which information this should be. Nevertheless, Article 5(3)'s underlying rationale and scholarly debate on informed consent make clear that companies are indeed obligated to disclose more detailed information regarding detection methods. In reality, game companies rarely provide more detailed information – if they provide any at all – in order to preserve trade secrets. Complicating matters further, there is no legal basis on which to ‘restrict’ the notion of informed consent in favor of trade secrets, resulting in a situation where game companies are essentially breaking the law. Despite its shortcomings, I have strongly argued in favor of consent’s central role in Article 5(3). Replacing or supplementing it with the legitimate interest or any other processing ground to address this issue is tempting, but runs counter to Article 5(3)'s underlying principles and would be too detrimental to transparency and autonomy. To reconcile these interests with game companies’ interests in preserving trade secrets, a novel use of a certification system to bridge the information gap was proposed. The proposed system results in only a small detriment to transparency and autonomy, and ultimately allows for the flow of information towards the user to be restricted.

The GDPR – at first glance – indirectly restricts usage of client-side anti-cheat through the right of access because records kept on players’ behavior are personal data (barring possibly the analytical component) and therefore subject to access requests. That personal data could potentially reveal sensitive information regarding detection methods or overall anti-cheat strategies. However, the GDPR explicitly recognizes that the right of access may be restricted if it adversely affects trade secrets. By employing Alexy’s law of balancing, it was asserted that there is sufficient legal basis to exclude any personal data which may reveal technologically sensitive information from access requests. Consequently, game companies are *not* restricted by the right of access to personal data in their usage of client-side anti-cheat.²⁷⁷

Raw materials	Personal data
Analytical component	May or may not qualify as personal data
End-result	Personal data

²⁷⁷ The proposed usage of certification, however, would allow users to indirectly verify the lawfulness of the processing via third party.

6.2 Limitations and recommendations for further research

This thesis played a pioneering role but many facets nevertheless remain unexplored. The following aspects in particular should be considered for future research:

1. The meaning of the term ‘necessary’ should be further explored and scrutinized. For example, if a game itself is badly designed in the sense that it is too easy to exploit, can it be considered truly necessary to deploy highly invasive anti-cheat to compensate for that shortcoming? And to what extent does Article 25 of the GDPR – data protection by design – factor into it?
2. The relationship between Article 7(4) of the GDPR and consent under Article 5(3) needs to be further explored. This article raises questions as to whether consent is freely given if providing the service depends on the processing of personal data which is not necessary for the performance of the contract. How should this provision be understood in the ePrivacy context?²⁷⁸
3. The question if (and if so, when) memory values or other bits of computer code processed to detect cheats constitute personal data, as this will dictate the extent of the GDPR’s applicability beyond the initial act of access.
4. The subject matter should be closely re-visited and further explored in light of the ePrivacy Regulation once a definitive version becomes available.
5. Further comparisons with other types of devices regulated by Article 5(3) (such as digital-rights management software).

More than anything else, however, future research should be focused on subjecting methods of detection to further legal analysis in conjunction with a more thorough technological understanding of the subject matter. My own research is limited (in addition to the limitations already mentioned in chapter one) due to the fact that I am first and foremost a legal scholar. I am apt enough to form a basic understanding required for legal analysis but cannot fully grasp the inner workings of detection mechanisms. Taking into account the lack of scholarly attention

²⁷⁸ If (certain types of) anti-cheat are not necessary for the service, then consent must be sought. But if that anti-cheat is not necessary for the service, the GDPR suggests such consent cannot be freely given. And does this only apply where the processing of personal data is concerned or also the access of terminal equipment as such? Once again, the choice to ‘import’ consent from the GDPR reveals its problematic nature.

and high complexity of the subject matter, I consider it unlikely that any legal scholar – at least on his or her own – would be able to tread in greater detail. What is necessary is collaboration between authors such as myself and authors such as Curda and Krutsko.²⁷⁹ Only then can the matter be explored in full detail and be given the attention it deserves.

6.3 Closing statement

So much of the debate surrounding Article 5(3) has been focused on cookies that it has seemingly been forgotten many other devices which interfere with users' terminal equipment exist, some of which far more invasive than cookies could ever be. Centering debate around the least invasive form of access is problematic because it risks more invasive forms getting an easy pass due to an underdeveloped system. Anti-cheat is a niche field, but many of the techniques used could see application outside of the online gaming context in the future. For example, in the wake of the 2016 United States elections, it has become increasingly clear that bots played at least some role in shaping public opinion through social media.²⁸⁰ There may come a time where social media platforms decide to start detecting these bots using client-side detection, and when that time comes, the legal framework needs to be properly thought out. The legislator's lack of guidance concerning key aspects, such as what constitutes '*necessary*' or '*strictly necessary*', is troubling. It is contradictory to on the one hand protect terminal equipment as part of the private sphere and rely on consent as the sole ground for lawfulness while on the other hand leaving the exemptions to that article undefined and up to wide interpretation. The decision to once again define consent in the ePrivacy Regulation proposal by simply referring to the GDPR further emphasizes this contradiction and lack of care. The case of client-side anti-cheat shows that consent essentially needs its own set of definitions and legal provisions in order to 'make sense' and be effective in that context. But seeing as how the ePrivacy Directive and Regulation '*particularize and complement*'²⁸¹ the DPD/GDPR and are intrinsically connected, we may

²⁷⁹ These authors wrote their theses on anti-cheat from a technology perspective.

²⁸⁰ According to a recent study conducted by Bessi and Ferrara, such bots were responsible for roughly one-fifth of the conversation surrounding the presidential election on Twitter. See: Alessandro Bessi and Emilio Ferrara, 'Social bots distort the 2016 US Presidential election online discussion.' (2016) 21(11) First Monday

²⁸¹ Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) [2017] Recital 5

wonder whether deviating from those instruments in one single, yet fundamental aspect²⁸² would even be possible. Other than the fact that users' terminal equipment *may* house personal data, Article 5(3) – which concerns itself with the *act* of intrusion into the private sphere – has very little in common with the DPD/GDPR and even the rest of the ePrivacy Directive/Regulation. There is no real value in itself to protecting information (as opposed to personal data) and this raises the question whether the inclusion of Article 5(3) in the ePrivacy instruments was a decision properly thought out.²⁸³ That is not to say an article like Article 5(3) should not be included in the law. On the contrary: the entirety of this thesis is essentially built on the conviction that our devices – similarly to our domiciles – are part of the private sphere and should be protected from intrusions as a matter of principle.²⁸⁴ Yet, by placing Article 5(3) into a legislative instrument where it is 'the odd man out' while simultaneously over-focusing the debate on cookies, its true potential in that regard is unlikely to ever be fully realized.

²⁸² I.e. consent.

²⁸³ Which of course raises the question where such an article should then be placed. This question is beyond this thesis's scope, however.

²⁸⁴ The argument of equating our devices with our domiciles is predominantly a principled argument; however, as chapter three (particularly paragraph 3.2) has shown, entering someone's device is essentially the 'first step' to being able to violate someone's privacy, and in this regard the value of Article 5(3) could be said to extend beyond a pure matter of principle.

BIBLIOGRAPHY

Article 29 Working Party, ‘Opinion 02/2010 on online behavioural advertising , WP171’ (2010)

Article 29 Working Party, ‘Opinion 4/2007 on the definition of consent, WP187’ (2007)

Article 29 Working Party, ‘Opinion 04/2012 on cookie consent exemption, WP194’ (2012)

Barnes W, ‘Rethinking Spyware: Questioning the Propriety of Contractual Consent to Online Surveillance’ (2006) 39 U.C. Davis Law Review 1545

Barosso and others, ‘Virtual Worlds, Real Money: Security and Privacy in Massively Multiplayer Online Games and Social and Corporate Virtual Worlds’ (2008) ENISA position paper

Berg and others, *Informed Consent: Legal Theory and Clinical Practice* (2nd edition, Oxford University Press 2001)

Bessi A and Ferrara E, ‘Social bots distort the 2016 US Presidential election online discussion.’ (2016) 21(11) First Monday

Blakley A F, Garrie D B and Armstrong M J, ‘Coddling Spies: Why The Law Doesn’t Adequately Address Computer Spyware’ (2005) 25(1) Duke Law & Technology Review

Blanke J, ‘“Robust Notice” and “Informed Consent.” The Keys to Successful Spyware Legislation’ (2006) 7(2) The Columbia Science and Technology Review 1

Bright P, ‘Valve DNS privacy flap exposes the murky world of cheat prevention’ (Ars Technica, 18 February 2014) <<https://arstechnica.com/gaming/2014/02/valve-dns-privacy-flap-exposes-the-murky-world-of-cheat-prevention/>> accessed on 2 February 2017

Bullock C E, ‘Informed Consent and Justified Hard Paternalism’ (PHD Thesis, University of Birmingham 2012)

Bygrave L A and Schartum D W, ‘Consent, Proportionality and Collective Power’ in Gutwirth and others (eds) *Reinventing Data Protection?* (Springer Science Business Media 2009)

Caltagirone and others, ‘Architecture for a Massively Multiplayer Online Role Playing Game Engine’ (2002) 18(2) Journal of Computing Sciences in Colleges 105

Cano N, *Game Hacking: Developing Autonomous Bots for Online Games* (No Starch Press 2016)

Castronova E, ‘On Virtual Economies’ (2002) 752 CESifo Working Paper 1

Chen and others, ‘Identifying MMORPG bots: a traffic analysis approach’ [2009] EURASIP Journal on Advances in Signal Processing - Special issue on signal processing applications in network intrusion detection systems 1

Chung and others, 'A Behavior Analysis-Based Game Bot Detection Approach Considering Various Play Styles' (2013) 35(6) ETRI Journal 1058

Chikhani R, 'The History Of Gaming: An Evolving Community' (*Tech Crunch*, October 31 2015) <<https://techcrunch.com/2015/10/31/the-history-of-gaming-an-evolving-community/>> accessed February 10 2017

Curda T, 'Analysis and detection of online game cheating software' (Bachelor thesis, Masaryk University 2004)

Desjardins J, 'The History and Evolution of the Video Games Market' (*Visual Capitalist*, January 11 2016)
<www.visualcapitalist.com/history-video-games-market/> accessed February 3rd 2017

Director Magazine, 'Trade Secrets of Business' (Director.co.uk, May 8 2016)
<<http://www.director.co.uk/news-trade-secrets-17924-2/>> accessed March 9 2017

Doyal L, 'Informed Consent: moral necessity or illusion?' (2001) 10(1) *Quality in Healthcare* 29

European Commission, 'Ex-Post REFIT evaluation of the ePrivacy Directive 2002/58/EC' (Commission Staff Working Document, 2017)

Fujita A, Itsuki H and Matsubara H, 'Detecting Real Money Traders in MMORPG by Using Trading Network' (Seventh Artificial Intelligence and Interactive Digital Entertainment Conference, Palo Alto, 2011)

Guest T, *Second Lives* (Hutchinson Random House 2007)

Heeks R, '*Understanding 'Gold Farming' and Real-Money Trading as the Intersection of Real and Virtual Economies*' (2010) 2(4) *Journal of Virtual Worlds Research* 3

Higginbotham S, 'People trust the internet but lie to it anyway' (Gigaom.com, November 27 2012)
<<https://gigaom.com/2012/11/27/people-trust-the-internet-but-lie-to-it-anyway/>> accessed March 9 2016

Hilven A and Woodward A, 'How safe is Azeroth, or, are MMORPGS a security risk?' (Proceedings of The 5th Australian Information Security Management Conference, Perth 2007)

Hoglund C and McGraw G, *Exploring Online Games: Cheating Massively Distributed Systems* (Kindle Edition, Pearson Education 2008)

Hussaini S, 'World of Warcraft Makers Continue Fight Against Bots'(American University Intellectual Property Brief, January 28 2009) <www.ipbrief.net/2016/01/28/world-of-warcraft-makers-continue-fight-against-bots/> accessed on February 10 2017

Hustinx P, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed GDPR' (2013) Collected Courses of the European University Institute's Academy of European Law (24th Session on European Union Law),

Hutchinson T, 'The Doctrinal Method: Incorporating Interdisciplinary Methods in Reforming the Law' (2015) 3 Erasmus Law Review 130

IAB Europe, 'Position on the Proposal for an ePrivacy Regulation' (2017) <http://iabireland.ie/wp-content/uploads/2017/03/20170328-IABEU-ePR_Position_Paper.pdf> accessed 7 March 2017

Indvik L, 'The Fascinating History of Online Role Playing Games' (*Mashable*, November 14 2012) <<http://mashable.com/2012/11/14/mmorpgs-history/#s.WRo96LVsqV>> accessed February 9 2017

Joshi R, 'Cheating and Virtual Crime in Massively Multiplayer Online Games' (Master thesis, University of London 2008) 59

Kang and others, 'Multimodal game bot detection using user behavioral characteristics' (2016) 5 SpringerPlus 523

Klang M, 'Spyware: paying for software with our privacy' (2010) 17(3) International Review of Law, Computers & Technology 313

Kosta E, *Consent in European Data Protection Law* (Martinus Nijhoff Publishers, 2013)

Krutsko D, 'Navigator – A scriptable software system for automating World of Warcraft' (Bachelor thesis, Carleton University 2013)

LaBossiere M, 'Forty Two Fallacies' (2002) <<https://aphilosopher.files.wordpress.com/2010/09/42-fallacies.pdf>> accessed 14 May 2017

Lastowska G, 'Rules of Play' (2009) 4(4) Games and Culture 379, 393

LawTeacher, 'Advantages And Disadvantages Of The Literal Rule Constitutional Law Essay' (Lawteacher.net 2013) <<https://www.lawteacher.net/free-law-essays/constitutional-law/advantages-and-disadvantages-of-the-literal-rule-constitutional-law-essay.php#ftn25>> accessed March 10 2017

Lehdonvirta V, 'Virtual Worlds Don't Exist: Questioning the Dichotomous Approach in MMO Studies' (2010) 10(1) Game Studies 1

Lehdonvirta V, 'Virtual Economics: Applying Economics to the Study of Game Worlds' (Conference on Future Play, East Lansing, 2005)

Lessig L, *Code and other laws of cyber space* (Basic Books 2006) 123

Malgieri G, 'Trade Secrets v. Personal Data: a possible solution for balancing rights' [2016] 6(2) International Data Privacy Law 102

McLeod I, *Legal Method* (3rd edition, MacMillan Press 1999)

McSherry C, 'A New Gaming Feature: Spyware' (*Electronic Frontier Foundation*, October 20 2005) <<https://www.eff.org/nl/deeplinks/2005/10/new-gaming-feature-spyware>> accessed 3 March 2017

Meisel A, 'The Exceptions to the Informed Consent Doctrine: Striking a Balance Between Competing Values in Medical Decision Making' [1979] 2 *Wisconsin Law Review* 413, 413

Mitterhofer and others, 'Server-Side Bot Detection In Massively Multiplayer Online Games' (2009) 7(3) *IEEE Security & Privacy* 1

Norman van G, 'Informed Consent: Respecting Patient Autonomy' in Van Norman and others (eds) *Clinical Ethics in Anesthesiology: A Case-Based Textbook* (Cambridge University Press 2011)

Olivetti J, 'Massively OP's Guide to MMO Business Models' (*Massively Overpowered*, April 30 2016) <<http://massivelyop.com/2016/04/30/massively-ops-guide-to-mmo-business-models/>> accessed February 11 2017

Schwarz N, 'Emotion, cognition and decision making' [2004] 14(4) *Cognition and Emotion* 433

Sheehan M, 'Can Broad Consent be Informed Consent?' (2011) 4(3) *Public Health Ethics* 226

Solove D J, 'Conceptualizing Privacy' (2002) 90(4) *California Law Review* 1087

Solove D J, "'I've Got Nothing to Hide" and Other Misunderstandings of Privacy' (2002) 44(1)

ANNEX A

Name	Conveyance	Content
<p>Hearthstone: Heroes of Warcraft²⁸⁵</p> <p>Heroes of the Storm²⁸⁶</p> <p>Overwatch²⁸⁷</p> <p>World of Warcraft²⁸⁸</p> <p>Diablo III²⁸⁹</p>	<p>Vehicle: Separate anti-cheat agreement.</p> <p>Visibility: The anti-cheat agreement is explicitly referred to when making a Battle.net (Blizzard’s online gaming platform) account.</p>	<p>In an effort to combat the efforts of those individuals who are willing to violate the EULA, Blizzard utilizes an ‘anti-cheating’ utility that runs as part of Blizzard games. This ‘anti-cheating’ utility performs limited scans of:</p> <p>the Random Access Memory (‘RAM’) that is occupied by a Blizzard game to confirm that the Blizzard game’s program has not been altered or ‘hacked’ in violation of the EULA;</p> <p>the Blizzard games ‘process’ to determine if any unauthorized third-party programs or computer code has been attached to the Blizzard games process;</p> <p>the Windows Process List to determine if any confirmed hacking, botting or cheating programs are presently open in violation of the EULA; and</p> <p>the Windows Handles list to see which processes have a handle to the Blizzard games ‘process’. Additional information obtained from RAM and/or disc for the processes that</p>

²⁸⁵ <http://eu.blizzard.com/en-gb/company/legal/anti-cheating.html>

²⁸⁶ <http://eu.blizzard.com/en-gb/company/legal/anti-cheating.html>

²⁸⁷ <http://eu.blizzard.com/en-gb/company/legal/anti-cheating.html>

²⁸⁸ <http://eu.blizzard.com/en-gb/company/legal/anti-cheating.html>

²⁸⁹ <http://eu.blizzard.com/en-gb/company/legal/anti-cheating.html>

		have a handle to the Blizzard games ‘process’ will be used to determine if it is a confirmed hacking, botting or cheating program in violation of the EULA.
Counterstrike: Global Offensive ²⁹⁰ Dota 2 ²⁹¹	Vehicle: Subscriber Agreement Visibility: The terms are long and the anti-cheat provisions are hidden away. Inclusion of the word ‘cheat’ does make it easier to locate via search.	Steam and the Content and Services may include functionality designed to identify software or hardware processes or functionality that may give a player an unfair competitive advantage when playing multiplayer versions of any Content and Services or modifications of Content and Services (“Cheats”). (...)Further, you acknowledge and agree that an online multiplayer host may report your use of Cheats to Valve, and Valve may communicate your history of use of Cheats to other online multiplayer hosts.
H1Z1 ²⁹²	Vehicle: Privacy policy Visibility: Users are confronted with the privacy policy when creating an account. The policy is well-ordered lay-out wise and uses indexation. Inclusion of the word ‘cheat’ makes it	Please note that, when running, some of our games may monitor your computer’s random access memory (“RAM”), media access control (“MAC”) address, configuration files and system files, etc., for unauthorized third party programs running concurrently with your game which, in Daybreak Games’ sole determination: (i) enable or facilitate cheating of any type; (ii) allow users to modify or hack the applicable Daybreak Games game interface, environment, and/or experience in any way not expressly authorized by Daybreak Games; or (iii) intercept, “mine” or otherwise collect information from or through the

²⁹⁰ http://store.steampowered.com/subscriber_agreement/

²⁹¹ http://store.steampowered.com/subscriber_agreement/

²⁹² https://www.daybreakgames.com/privacy?locale=en_US

	<p>easier to locate via search.</p>	<p>applicable Daybreak Games game (each, an “Unauthorized Third Party Program”). In the event that a Daybreak Games game detects an Unauthorized Third Party Program, (a) the Daybreak Games game may communicate information back to Daybreak Games, including without limitation, your Daybreak Games account username, details about the Unauthorized Third Party Program detected and the activities or functions performed thereby, and/or details about your computer (...).</p>
<p>Guild Wars 2²⁹³</p>	<p>Vehicle: Subscriber Agreement</p> <p>Visibility: The terms are long and the anti-cheat provisions are hidden away. No mention is made of the word ‘cheat’ or anything close to it. No indexation, however, the provisions are filed under ‘Privacy and data protection’ which is at least indicative.</p>	<p>ArenaNet HAS THE RIGHT, BUT NO OBLIGATION, TO MONITOR OPERATION OF ANY SERVICE, CONTENT OR GAME AT ANY TIME AND IN ANY MANNER, INCLUDING BUT NOT LIMITED TO MONITORING COMMUNICATIONS AND COMMUNICATIONS INTERFACES, STORAGE DEVICES, RANDOM ACCESS MEMORY, OR CPU PROCESSES RELATED TO HARDWARE YOU USE WITH THE GAME. SUCH MONITORING MAY ALSO INCLUDE, BUT IS NOT LIMITED TO, MONITORING FOR THE PURPOSES OF DETECTING THE GAME UNDER SECTION 8(c) or 8(e). YOU CONSENT TO THE FOREGOING MONITORING AND ACKNOWLEDGE THAT ArenaNet MAY, AT ANY TIME, AND IN ANY MANNER, COMMUNICATE</p>

²⁹³ <https://www.guildwars2.com/en/legal/guild-wars-2-user-agreement/>

		ANY INFORMATION BETWEEN HARDWARE YOU USE WITH THE GAME AND ANY MECHANISM ArenaNet MAY CHOOSE FOR SUCH COMMUNICATIONS.
Runescape ²⁹⁴	<p>Vehicle: Privacy policy</p> <p>Visibility: The terms are long and there is no indexation.</p>	We generate and store logs indicating usage of the Jagex Products such as activity in our games and public and private chat communications. This includes monitoring play patterns and anti-tamper checks which verify the correct internal operation of our software and are designed to spot abusive or inappropriate activities. (...)The information we collect may be used: (...)To enforce our terms and conditions, and prevent or detect hacking activities, security breaches or safety risks in connection with our websites and Jagex Products.
The Elder Scrolls Online ²⁹⁵	<p>Vehicle: Privacy policy</p> <p>Visibility: While the terms are long, the word ‘anti-cheat’ is at least used, making it easier to find.</p>	<p>Generally, we may or our service providers may use the information we collect to provide our services to you; (...) assist in security and fraud prevention; for system integrity (preventing hacking, cheats, spamming, etc.)</p> <p>In an effort to provide a safe and fair gaming environment to players of its games, and to protect against payment fraud, ZeniMax employs “anti-cheating” and fraud prevention software or applications during the use of certain online products and services to prevent fraudulent activities and behavior that may negatively affect the experiences of a player,</p>

²⁹⁴ <https://www.jagex.com/terms/privacy>

²⁹⁵ https://www.zenimax.com/legal_privacy_us

		<p>some of which may be operated by third party providers.</p> <p>We may collect personal information during: Anti-cheat and fraud prevention and detection.</p>
<p>Black Desert Online²⁹⁶²⁹⁷</p>	<p>Vehicle: Privacy Policy</p> <p>Visibility: Mostly hidden away in the privacy policy. No commonly expected terms are used.</p>	<p>During your gameplay, we will collect your session information, including your IP address, your MAC address, your hardware information, the time your session begun, how long it lasted, how and when it ended.</p> <p>This information is used in order to:</p> <ul style="list-style-type: none"> • provide you customer support when you request it; • verify that you do not violate the terms of service; • generate anonymous statistics about our player base; • improve the game experience.
<p>Darkfall: Rise of Agon²⁹⁸</p>	<p>Vehicle: Terms of Service</p> <p>Visibility: Hidden away in the privacy policy. Appears under ‘Active Game and Account Monitoring’.</p>	<p>You agree that Big Picture Games may use whatever procedures or protocols it may deem necessary to monitor your computer and activity in the Game and the World. This may include, but is not limited to, monitoring your personal computer to determine the validity of your installation, your account and the Game and to assure that you are not using any third party software that might violate these TOS or the EULA.</p>

²⁹⁶ <https://www.blackdesertonline.com/legal/privacy-policy>

²⁹⁷ <https://www.unknowncheats.me/forum/anti-cheat-bypass/125231-dll-injection-xigncode.html>

²⁹⁸ <https://www.darkfallriseofagon.com/legal-info/tos-eula/>

Path of Exile ²⁹⁹	Anti-cheat provisions are absent.	-
SMITE ³⁰⁰	Vehicle: End User License Agreement Visibility: Hidden away in the EULA. Appears under ‘CONSENT TO MONITOR.’	IN ADDITION, THE SOFTWARE PRODUCT AND ANY RELATED HI-REZ SERVICES MAY MONITOR EACH OF YOUR HARDWARE DEVICE'S RANDOM ACCESS MEMORY (RAM) FOR UNAUTHORIZED THIRD PARTY PROGRAMS RUNNING CONCURRENTLY WITH THE SOFTWARE PRODUCT.

Name	Conveyance	Content
Easy Anti Cheat ³⁰¹	Privacy policy. Very visible.	The policy is very elaborate and aims to be transparent. It supplies the user with lots of information and provides easy to follow clarification and explanations. It even goes so far as to instruct users how they can verify the software does not run when the game is closed.
BattleEye ³⁰²	Privacy policy. Very visible.	<i>‘While BattlEye needs to have full access to your system’s internals to have the</i>

²⁹⁹ <http://www.ownedcore.com/forums/mmo/path-of-exile/poe-bots-programs/508787-warning-anti-cheat-implemented-stop-using-any-hack-bot-proof-inside-24.html>

³⁰⁰ <https://www.hirezstudios.com/wp-content/themes/hi-rez-studios/pdf/smite-end-user-license-agreement.pdf>

³⁰¹ <https://support.easyanticheat.net/kb/privacy/?lr=en-us>

³⁰² <https://www.battleeye.com/privacy-policy/>

		<p><i>capability to detect all hacks (...)</i> The policy indicates that it may <i>'transmit flagged executable code to our servers for further review'</i> and that no other memory contents are transmitted to the BattlEye servers. Aside from this information, nothing else is mentioned or explained. The fact that BattlEye runs in kernel mode is omitted.</p>
ESEA Client ³⁰³	Privacy policy. Very visible.	<p>Terminology is extremely vague (<i>'information from your computer that ESEA deems reasonably necessary'</i>), although some examples of techniques are mentioned. Usage of kernel-mode is omitted.</p>

³⁰³ https://play.esea.net/index.php?s=content&d=privacy_policy

ANNEX B: INTERVIEW WITH PARTICIPANT #1



Your expertise on Warden, bots, and other matters

8 messages

Ruben Greidanus

Mon, Jan 9, 2017 at
11:43 AM

To: *****@*****.com

Hello ***,

My name is Ruben Greidanus, I'm currently writing a master's thesis on the legality of bot-detection methods; both client and server side. I read your blog on Warden and found it a very interesting read. I am somewhat knowledgeable on bots and how detection works but some areas are still quite lacking. Would you be willing to answer some of my questions (mainly technical in nature) somewhere in the near-future? These questions would mainly deal with:

- MMORPG functionality (client-server architecture)
- Bot functionality (how do they interact with the game, etc)
- Detection methods (which techniques are currently being employed, etc)
- And how the above relates to one another.

I would ask you the questions through e-mail so that you can answer them at your own leisure. I will of course credit you as my source, or keep your name anonymous if that's what you prefer. I look forward to hearing from you.

Kind regards,

Ruben Greidanus

*** <*****@*****.com>

Mon, Jan 9, 2017 at 12:47 PM

To: Ruben Greidanus <r.greidanus@tilburguniversity.edu>

Hello!

I have not specifically reverse engineered Warden since 2008 or 2009 (when they threatened a lawsuit), but to my knowledge it still works largely the same way. If you're looking for someone with knowledge of which types of scans are present in the current version of Warden, I'm not your man. :)

I am otherwise happy to answer questions on these topics. Thanks for your e-mail, have a good day!

*** ***** , LLC

[Quoted text hidden]

Ruben Greidanus <r.greidanus@tilburguniversity.edu>

Mon, Jan 9, 2017
at 1:15 PM

To: *** <*****@*****.com>

Hi ***,

Thanks for your swift reply. I don't have to know exactly what kind of scans are currently present in Warden, it's more about the tools that game developers theoretically have available to them. I'm more so looking for a person with a lot of

general knowledge and know-how on this subject, and from what I've been reading I definitely think you fit the bill. I really appreciate your willingness to help me out with this! I'll send you some questions in the coming weeks.

Kind regards,

Ruben Greidanus

[Quoted text hidden]

Ruben Greidanus <r.greidanus@tilburguniversity.edu>

Fri, Jan 27, 2017 at
10:35 PM

To: *** <*****@*****.com>

Hi ***,

As discussed, I have several questions that I would love to get your thoughts on. Just to quickly summarize what I'm trying to do: I want to provide an overview of common client-side and server-side bot-detection methods and see how these relate to the European Union privacy & data protection legal framework. So it's not my intention to prove that Blizzard invades users' privacy or anything like that. I'm more interested in a general, theoretical perspective.

In any case, this is my understanding so far:

Detection methods either take place client or server-side. Client-side methods may involve:

1. Monitoring the game memory space through signature based detection. Similar to the way in which virus scanners work.
2. Hash validation in the game memory space. Specific areas of the memory are

targeted and are compared to an original, 'clean' version.

3. Process-list scanning, running processes are compared to a blacklist.

4. Window title-scanning, titles are compared to a blacklist.

My first, most general question is to what extent is the above correct and are any notable methods that I've left out? I'm trying to create some kind of typology/categorization, but I'm not sure whether that's actually possible or if there's so many, vastly different methods, that trying to categorize them is impossible.

My second question. Could method 1 & 2 also be used to scan outside of the game process? I read that very old-school anti cheat detection such as Punkbuster actually applies these methods to the entire memory space, is this indeed possible?

Furthermore, is it correct that in order to scan outside the game process, anti-cheating software would need to run in 'kernel mode' rather than 'user mode'? In other words, is it correct that anti-cheating software can only scan inside the game process **unless** it's running in kernel mode?

Furthermore, is my understanding correct that method 2 would be used to identify, for example, injected code or function hooks inside the game process?

Lastly, you talk about method 3 & 4 on your blog. If I understand correctly: Warden used to employ these in the past. It used to work in that it had a blacklist of hashes. It assessed the running processes / window titles on the player computer and compared the result to the blacklist. In Warden's case, the only thing that was sent back was either a 'yes' or 'no'. Was it Warden that converted the actual process name or windows title into a hash or are these hashes available by default? Did Warden ever come into contact with the actual name of a process or window title? And once again, is it even possible for Warden to scan other processes or window titles when it's not running in Kernel mode?

I hope I'm making sense here, I have no doubt I'm using some of the terms incorrectly. Thanks again for your time and I look forward to hearing from you.

Kind regards,

Ruben Greidanus

[Quoted text hidden]

*** <*****@*****.com>

Fri, Feb 3, 2017 at 4:36 PM

To: Ruben Greidanus <r.greidanus@tilburguniversity.edu>

My apologies, I had started drafting a reply and got pulled away.

1. Monitoring the game memory space through signature based detection. Similar to the way in which virus scanners work.
2. Hash validation in the game memory space. Specific areas of the memory are targeted and are compared to an original, 'clean' version.
3. Process-list scanning, running processes are compared to a blacklist.
4. Window title-scanning, titles are compared to a blacklist.

My first, most general question is to what extent is the above correct and are any notable methods that I've left out? I'm trying to create some kind of typology/categorization, but I'm not sure whether that's actually possible or if there's so many, vastly different methods, that trying to categorize them is impossible.

This is generally accurate.

My second question. Could method 1 & 2 also be used to scan outside of the game process? I read that very old-school anti cheat detection such as Punkbuster actually

applies these methods to the entire memory space, is this indeed possible?

Furthermore, is it correct that in order to scan outside the game process, anti-cheating software would need to run in 'kernel mode' rather than 'user mode'? In other words, is it correct that anti-cheating software can only scan inside the game process **unless** it's running in kernel mode?

#1 and #2 can scan outside of the game process, without kernel mode. All it would technically need is the ability to use ReadProcessMemory on the target process, which may require running "as Administrator" but certainly still available in user mode.

Furthermore, is my understanding correct that method 2 would be used to identify, for example, injected code or function hooks inside the game process?

#2 is a way to check for any modifications, which would include injected code/function hooks as well as simple hacks, like run speed modifications and such.

Lastly, you talk about method 3 & 4 on your blog. If I understand correctly: Warden used to employ these in the past. It used to work in that it had a blacklist of hashes. It assessed the running processes / window titles on the player computer and compared the result to the blacklist. In Warden's case, the only thing that was sent back was either a 'yes' or 'no'. Was it Warden that converted the actual process name or windows title into a hash or are these hashes available by default? Did Warden ever come into contact with the actual name of a process or window title? And once again, is it even possible for Warden to scan other processes or window titles when it's not running in Kernel mode?

Warden was doing the hashing, using a standard algorithm though I do not recall which. Probably SHA.

Warden comes into contact with the names because that is what the Windows API provides, anyone can do it -- EnumWindows + GetWindowText. EnumProcesses, you can even tell what DLLs are loaded in a process with EnumProcessModules. Many games use these methods. WoW has used these to scan for hacks before you even log in (probably still does) and warns the user if it finds a known problem (e.g. a known keylogger/trojan targeting WoW accounts).

However, some of these API are restricted by user permissions in Windows. For example, attempting to EnumProcessModules on an Administrator-level (elevated) process may fail from a Standard-level (non-elevated) process. So their expected benefit is already lessened due to security in Windows. For this and similar reasons, many anti-cheat systems do choose to use kernel mode, which is not subject to this restriction.

*** *****, LLC

[Quoted text hidden]

Ruben Greidanus <r.greidanus@tilburguniversity.edu>

Sun, Feb 12, 2017
at 5:59 PM

To: *** <*****@*****.com>

Hi ***,

No problem, sorry for my late reply as well, could have sworn I hit 'send' last weekend but I just noticed my reply was still under drafts. Thanks for your answers, it has been extremely valuable in getting a better grasp on all the technical stuff. I'll receive some feedback from my supervisors soon and I may have some additional questions after that, if that's all right with you of course.

By the way, I'm very curious if you know more about the following. On botting/cheating forums I constantly see people reference a lawsuit that Blizzard was allegedly involved in where the Courts told them they were not allowed to scan outside the memory space occupied by their games. This would constitute a privacy violation, presumably. Some people also say this is why they stopped scanning window titles and so forth. I've scoured the entire internet for such a lawsuit but I've been unable to find it. Everyone seems to talk about it but no one actually knows or mentions what this case was called or when it can be found. I don't think it's MDY Industries/Glider v. Blizzard as that seems to relate to copyright infringement mainly.

Any ideas?

Kind regards,

Ruben

[Quoted text hidden]

*** <*****@*****.com>

Mon, Feb 13, 2017 at 7:21 PM

To: Ruben Greidanus <r.greidanus@tilburguniversity.edu>

MDY v Blizzard did not put any such restrictions on Warden, and I'm not aware of a case that did.

If they stopped using a scan for window titles, it's probably because people worked around the scan anyway. I mean, once you know it's there, you just change the window title, right?

[Quoted text hidden]

Ruben Greidanus <r.greidanus@tilburguniversity.edu>

Wed, Feb 15, 2017 at
10:22 AM

To: *** <*****@*****.com>

Hi ***,

Thanks, and yes I was thinking the same thing. I'm going to assume it's just a myth that gets repeated from person to person without an actual source.

Kind regards,

Ruben

[Quoted text hidden]

ANNEX C(1): INTERVIEW WITH PARTICIPANT #2

[2/9/2017 1:48:00 AM] *** Participant #2 would like to add you on Skype

Hi Ruben, I'd like to add you as a contact. ***

[2/12/2017 9:18:48 PM] *** Ruben has shared contact details with Participant #2 . ***

[2/12/2017 9:58:02 PM] Ruben: Hi Participant #2, thanks for taking the time to meet me!

[2/12/2017 9:58:26 PM] Participant #2 : Sure thing.

[2/12/2017 9:58:36 PM] Ruben: Want to get right into it?

[2/12/2017 9:58:43 PM] Participant #2 : Sure

[2/12/2017 9:59:38 PM] Ruben: All right so that thesis you sent me was super helpful. I'm basically looking at client-side detection methods and I'm trying to think of a general categorization of sorts.

[2/12/2017 10:00:14 PM] Participant #2 : Do you prefer to type things out or voip?

[2/12/2017 10:00:41 PM] Ruben: I would prefer to type things out, my English is fine but this way I can organize my thoughts better if that's all right?

[2/12/2017 10:00:48 PM] Ruben: And I have a terrible Dutch accent .

[2/12/2017 10:00:49 PM] Participant #2 : Sure.

[2/12/2017 10:01:48 PM] Ruben: All right so basically, from what I understand you have:

1. Monitoring the game memory space through signature based detection. Similar to the way in which virus scanners work. Can also be used on the rest of the computer memory.
2. Hash validation in the game memory space. Specific areas of the memory are targeted and are compared to an original, 'clean' version. Can also be used on the rest of the computer memory.
3. Other methods such as calling an active process-list or window titles, with functions like EnumWinTitles

[2/12/2017 10:02:00 PM] Ruben: And then finally there's these oddball methods like Punkbuster which make screenshots of your computer (allegedly).

[2/12/2017 10:02:12 PM] Ruben: Out of the things I've mentioned is there any obvious technique or method that I'm missing?

[2/12/2017 10:03:26 PM] Participant #2 : So keep in mind that, at least for non-kernel anti-cheats, they can't really scan "the rest of computer memory"

[2/12/2017 10:04:20 PM] Participant #2 : In Windows (and OSX) they might be able to see that an application has an open handle to the game but if the application is running with escalated

privileges, the anti-cheat would not be able to read the memory of that application. Furthermore, doing so would violate privacy laws in some countries.

[2/12/2017 10:04:53 PM] Ruben: Yeah so in layman's terms that's basically running something in administrator mode you mean right?

[2/12/2017 10:04:56 PM] Ruben: Administrator mode = elevated.

[2/12/2017 10:05:08 PM] Participant #2 : Yes, unless the game is running in admin mode as well for some reason.

[2/12/2017 10:05:43 PM] Participant #2 : And as far as I know, CreateToolhelp32Snapshot is the most popular function anti-cheats use.

[2/12/2017 10:06:23 PM] Participant #2 : Call of Duty I heard takes screenshots of suspected computers. Since Activision/Blizzard is the same company, I would not be surprised if Overwatch takes screenshots as well.

[2/12/2017 10:06:59 PM] Participant #2 : However, I don't know if they take a screenshot of the computer or just what the game is rendering. So it could be that external overlays aren't captured by the screenshots.

[2/12/2017 10:07:12 PM] Ruben: Gotcha, interesting.

[2/12/2017 10:07:31 PM] Ruben: Would you say the list i just sent is generally accurate? in that it provide a rough overview of what's currently available?

[2/12/2017 10:07:51 PM] Ruben: Taking into account of course that many specific techniques will remain secret as that in game developers best interest.

[2/12/2017 10:08:11 PM] Participant #2 : That's a good starter list but there are a lot of ways you could detect bots

[2/12/2017 10:09:45 PM] Participant #2 : For example, you could detect people reading your memory like Overwatch does by allocating memory that never gets used (which means windows doesn't allocate physical ram) but then if something accesses it (like a bot) then windows allocates physical ram, and the game would see that that memory was read/accessed.

[2/12/2017 10:10:09 PM] Ruben: So that's sort of a trap?

[2/12/2017 10:10:35 PM] Participant #2 : Here's a whole thread on that:
<https://www.unknowncheats.me/forum/overwatch/177750-overwatch-crashes-readprocessmemory.html>

[2/12/2017 10:10:42 PM] Participant #2 : And a sample implementation:
<https://gist.github.com/d/d6118638b0ef711b30bfcfe5b083d067>

[2/12/2017 10:12:06 PM] Participant #2 : Other detection methods include checking for debuggers, which I sent you a comprehensive link about before.

[2/12/2017 10:12:16 PM] Ruben: Interesting, seems like the possibilities are basically endless right? just depends on how creative the companies get?

[2/12/2017 10:12:24 PM] Participant #2 : Yep, basically.

[2/12/2017 10:12:30 PM] Ruben: I read about valve checking users' dns caches for known cheat drm-servers a couple of years ago.

[2/12/2017 10:12:33 PM] Ruben: Also found that very creative.

[2/12/2017 10:12:43 PM] Participant #2 : And it's not just about detecting bots but also protecting your code against bots.

[2/12/2017 10:12:59 PM] Ruben: What do you mean by protecting your code?

[2/12/2017 10:13:10 PM] Participant #2 : They don't anymore, but they did do that to catch a kernel based hack

[2/12/2017 10:13:41 PM] Participant #2 : For example, Overwatch encrypts their binary so that you can't just drop it into IDA Pro and perform static analysis.

[2/12/2017 10:14:06 PM] Participant #2 : When you run the game, it uses what's known as a TLS Callback to set up exceptions which decrypt the binary and run the game.

[2/12/2017 10:14:25 PM] Participant #2 : It also uses countless anti-debugging methods to prevent people from debugging the game.

[2/12/2017 10:14:49 PM] Ruben: So they basically try to stop people from reverse engineering their software right?

[2/12/2017 10:15:00 PM] Participant #2 : That memory "trap" I was talking about is another way to protect your code (And detect bots).

[2/12/2017 10:15:04 PM] Participant #2 : Yes.

[2/12/2017 10:15:17 PM] Ruben: Gotcha.

[2/12/2017 10:15:26 PM] Ruben: Seeing as we're already talking about kernel mode, I also have some questions about that.

[2/12/2017 10:16:14 PM] Participant #2 : Another way to protect code is decrypting code on the fly, just before it get's ran, as well as having bogus code that never gets run but the disassembler thinks is real code.

[2/12/2017 10:16:38 PM] Participant #2 : The Denuvo copy-protection system uses this, and many other techniques, to prevent piracy of games such as Doom.

[2/12/2017 10:16:43 PM] Participant #2 : Sure.

[2/12/2017 10:17:04 PM] Ruben: Interesting, yeah there are lots of similarities between digital rights management software and this.

[2/12/2017 10:17:06 PM] Ruben: If I understand correctly, anti-cheat software cannot overrule Windows security privileges which may mean that it can't read another process memory space. So, for that reason, some anti-cheat software runs in kernel mode. How is this achieved, exactly? Is this something that the user has to allow? How do you force something to run in kernel mode?

[2/12/2017 10:19:49 PM] Participant #2 : Yeah, you have to understand that anti-cheats are running in a hostile environment where the hacker has the upper hand.

[2/12/2017 10:22:02 PM] Participant #2 : They control every aspect of their computer, and software like VAC sometimes denies people access because their systems are configured in an "insecure" fashion such as disabling DEP.

[2/12/2017 10:22:50 PM] Participant #2 : As for running code in kernel-mode, it's basically a driver. Like a keyboard driver or a video card driver. So hackers (or anti-cheat developers) write a driver which the user has to allow and install.

[2/12/2017 10:24:46 PM] Participant #2 : The thing about drivers though is that they have to be signed by a certificate. So either you go and pay a CA (certificate authority) to sign your driver or you somehow get the user to install your certificate so the driver can install themselves. If you want to run drivers without signing them then you have to enable "test mode" in windows which means that anti-cheat systems like VAC can detect that and deny you access, like they do when you disable DEP.

[2/12/2017 10:25:16 PM] Ruben: Right, so that's basically a dead giveaway that you're trying to hide something

[2/12/2017 10:25:35 PM] Ruben: Kind of in the same way that running in a virtual machine may seem suspicious

[2/12/2017 10:25:51 PM] Participant #2 : Yes, but I still think that people can see what drivers are installed on your computer, so I'm not sure if that's the safest way to go either.

[2/12/2017 10:26:23 PM] Participant #2 : But regardless, if your anti-cheat is kernel based, then they have access to the entire computer and can read memory easily.

[2/12/2017 10:26:35 PM] Participant #2 : Yes, Overwatch prevents you from running in a virtual machine

[2/12/2017 10:26:48 PM] Ruben: And I would assume that anti cheat will usually get their drivers signed?

[2/12/2017 10:26:56 PM] Participant #2 : Although I heard that it works fine in Wine which is weird.

[2/12/2017 10:27:13 PM] Participant #2 : Yes, kernel anti-cheats will always sign their stuff officially

[2/12/2017 10:27:19 PM] Participant #2 : Just like Blizzard sign's their executables

[2/12/2017 10:27:42 PM] Participant #2 : You can right click an exe and click on Digital Signatures to see it

[2/12/2017 10:28:06 PM] Ruben: Right, could such a driver installation be included in a game-installation itself? so hypothetically, i install an mmo and in addition to installing the binaries it also places this driver?

[2/12/2017 10:28:10 PM] Ruben: Or is it always a separate process

[2/12/2017 10:29:17 PM] Participant #2 : Yes, you will get a special dialog box though to install the driver

[2/12/2017 10:29:35 PM] Ruben: Interesting, I wonder how many users actually realize what's they're consenting to then

[2/12/2017 10:29:39 PM] Participant #2 : It sometimes looks like this: <http://www.ross-tech.com/vag-com/usb/V64-Driver-7.png>

[2/12/2017 10:29:58 PM] Participant #2 : Search "install driver dialog" to see more examples

[2/12/2017 10:30:23 PM] Ruben: Now, suppose, what if both cheating software and anti-cheating software run in kernel mode. How does this pan out, how does this change the whole detection approach?

[2/12/2017 10:31:16 PM] Participant #2 : I'm not too familiar with kernel-mode but I would assume it's the same way as non-kernel-mode

[2/12/2017 10:31:46 PM] Ruben: It's just that now the anti-cheating software can look anywhere it wants without (technical) limitations?

[2/12/2017 10:32:15 PM] Participant #2 : Yeah basically, they could probably see the list of loaded drivers, scan any process they want

[2/12/2017 10:32:41 PM] Participant #2 : But I'm not sure how easy it would be for them to read the memory of the kernel-mode hack

[2/12/2017 10:32:48 PM] Participant #2 : I don't know how that whole business works.

[2/12/2017 10:33:13 PM] Ruben: No worries, things are already way more clear than they were before.

[2/12/2017 10:34:01 PM] Ruben: *****. I have some very basic experience with making pixel reading bots.

[2/12/2017 10:34:25 PM] Ruben: Why do you reckon they're not used more often? Is it just too limited in comparison to advanced techniques like memory manipulation and code injection?

[2/12/2017 10:34:45 PM] Participant #2 : So yeah I mean it worked well enough, it might work better now since they opened up their api just a bit but nothing too crazy

[2/12/2017 10:35:26 PM] Participant #2 : Pixel bots? they work great for aimbots in overwatch

[2/12/2017 10:36:08 PM] Participant #2 : For wow, it depends what you're doing but if you're doing it through an addon or whatever then Blizzard can probably detect that like they did with Pirox back in the day.

[2/12/2017 10:36:36 PM] Participant #2 : But most of the time you can't really get enough information out of it like you can with memory reading. For example, you can't write an ESP wall hack in Overwatch using pixel bots. you have to read memory.

[2/12/2017 10:37:11 PM] Ruben: Gotcha. i would also imagine that executing loads of different tasks through pixel reading would eat up a lot of processing power. is that correct?

[2/12/2017 10:37:20 PM] Ruben: If I remember correctly, scanning the screen constantly requires quite a bit?

[2/12/2017 10:38:02 PM] Participant #2 : Um it's about the same.

[2/12/2017 10:39:12 PM] Participant #2 : Reading the screen is kinda slow if you're using the standard bitblt technique, but if you're using a driver or something then it's fast. It's about 20ms per screenshot if you're reading the whole screen of the game. Slow....

[2/12/2017 10:39:56 PM] Participant #2 : Reading memory is also slow, if you're using ReadProcessMemory. I solved this technique by using memory caching algorithms. But it's nowhere near as fast as injecting a DLL and reading memory directly or using a kernel.

[2/12/2017 10:40:06 PM] Participant #2 : Kernel-driver I mean.

[2/12/2017 10:40:20 PM] Ruben: I didn't even know it was possible through drivers

[2/12/2017 10:40:27 PM] Participant #2 : Regardless, performance isn't really the issue here.

[2/12/2017 10:40:45 PM] Participant #2 : Driver screen reading is how I think most of these screen recorders are written.

[2/12/2017 10:41:11 PM] Participant #2 : Like camtasia I think. Fraps injects a DLL.

[2/12/2017 10:41:42 PM] Participant #2 : And hooks to the DirectX endscene function to record the screen. So yes screen reading can be done by injecting DLL's or using kernel-drivers, just like reading memory.

[2/12/2017 10:43:04 PM] Ruben: Interesting, im sure you would laugh at the 'bots' (more like macros i guess) ive made in the past hahah, total mess. so many things i wasnt aware of

[2/12/2017 10:43:16 PM] Ruben: Moving on, would you say that

[2/12/2017 10:43:55 PM] Ruben: If a game is really well designed, and relies on a client-server architecture like an mmo, then traditional cheating (and by that i mean things like speedhacks etc) is basically impossible?

[2/12/2017 10:44:59 PM] Participant #2 : Yes, unless the game was designed poorly (like conan). I tried speed hacking in wow once, you move quickly sure but spells arn't going to be cast quickly.

[2/12/2017 10:46:25 PM] Participant #2 : But I've seen some creative hacks in the past for games like wow, where you could mountain climb, etc. Basically it's all about how much stuff is done at the client level. I think physics is done client side which means people modified the game world to collect herbs easier, but herbs were still spawned server side.

[2/12/2017 10:46:57 PM] Ruben: I see.

[2/12/2017 10:47:12 PM] Participant #2 : here's a video you should watch from the guy that made Glider back in the day: https://www.youtube.com/watch?v=hABj_mrP-no

[2/12/2017 10:47:44 PM] Ruben: Hah yes I've watched this video actually, it was one of the first things i found. I'm definitely going to re-visit it now that i understand things more.

[2/12/2017 10:48:05 PM] Ruben: Two questions left,

[2/12/2017 10:48:19 PM] Ruben: What are your thoughts on server-side detection methods, especially in contrast with client-side?

[2/12/2017 10:48:43 PM] Ruben: A lot of articles are being published about them in academia and the authors generally tout them as a superior alternative to anything client side

[2/12/2017 10:48:47 PM] Participant #2 : They're fairly effective because you never really know what they're doing. Like credit card scams

[2/12/2017 10:49:04 PM] Participant #2 : I remember reading that if you fill up two cans of gas and buy cigarettes, it disables the credit card.

[2/12/2017 10:49:37 PM] Participant #2 : Same type of business happens in server-side detection, like they do with movement in wow. It prevents you from teleporting, except for small distances.

[2/12/2017 10:50:40 PM] Participant #2 : But systems like VAC and warden are also designed to send client-side detection code at any time. So there could, for example, be 20 different detection modules, but your computer would only receive 2. That prevents hackers from getting all the detection code at the same time.

[2/12/2017 10:51:09 PM] Ruben: That's clever.

[2/12/2017 10:51:33 PM] Participant #2 : I know those serial number protected programs do the same thing

[2/12/2017 10:51:47 PM] Participant #2 : They only provide part of the validation code, new versions introduce another part.

[2/12/2017 10:51:58 PM] Participant #2 : I think it's called partial serial number validation or something

[2/12/2017 10:52:29 PM] Participant #2 : The whole point is, if the code is accessible, hacker will figure it out, if it isn't then they have no way to figure it out.

[2/12/2017 10:53:10 PM] Participant #2 : But remember that server-side detection can only do so much, it can't, for example, detect the hacks you're running client-side, which means you want to use both techniques to have an effective anti-cheat.

[2/12/2017 10:53:28 PM] Participant #2 : Not that it matters though because hackers just get smarter and smarter.

[2/12/2017 10:53:34 PM] Participant #2 : (Look at Korea lol)

[2/12/2017 10:54:01 PM] Ruben: Haha, yes. By the way, would you also say that server-side detection methods are probably inhibited by processing power? Seems like running that much behavioral analysis on player may be quite intensive.

[2/12/2017 10:54:26 PM] Ruben: Depends on how complicated the analysis is of course.

[2/12/2017 10:54:35 PM] Participant #2 : Yes, you can't do insane detection, like imagine wow running crazy analysis, their servers would die

[2/12/2017 10:55:09 PM] Participant #2 : However, as computers become faster, more and more possibilities open up. And sometimes they might only have to run intensive detection on a few "suspected" players instead of every player.

[2/12/2017 10:55:22 PM] Ruben: Ah yes that's true.

[2/12/2017 10:55:26 PM] Ruben: Hadn't considered that.

[2/12/2017 10:55:38 PM] Participant #2 : We've seen this before with proection systems

[2/12/2017 10:55:55 PM] Participant #2 : Denuvo wan't possible 10 years ago because encryption was expensive, now it doesn't matter. Thanks NSA :-)

[2/12/2017 10:56:06 PM] Ruben: Haha

[2/12/2017 10:56:38 PM] Participant #2 : At some point I feel it'll just become AI vs. AI though.

[2/12/2017 10:57:19 PM] Participant #2 : Reverse engineering might become impossible one day because of how complicated applications become, which means people will start writing AI's and complicated algorithms to reverse engineer applications for them. It'll be interesting what happens then.

[2/12/2017 10:57:55 PM] Participant #2 : I mean even right now we're seeing people give up on reverse engineering functions and just running the game's functions themselves... It'll just keep evolving and there will be new detection methods for those.

[2/12/2017 10:58:01 PM] Participant #2 : It's a cat and mouse game

[2/12/2017 10:58:16 PM] Ruben: Yeah and that's what makes it super interesting.

[2/12/2017 10:58:27 PM] Ruben: You mentioned by the way, in your first pm on ownedcore

[2/12/2017 10:59:09 PM] Ruben: You try to simulate human key presses and mouse presses as much as possible - but even those can be detected. you linked an article which (if i understand correctly) allows you to circumvent the flag that such inputs were injected.

[2/12/2017 10:59:29 PM] Participant #2 : Yeah using a driver :-P

[2/12/2017 10:59:31 PM] Ruben: If developers are able to see the origin of such inputs, why haven't way more people been banned? I've used autoit for years in games and never once did i receive a ban

[2/12/2017 10:59:56 PM] Participant #2 : So I think Overwatch did detect that at one point and ignored those types of inputs

[2/12/2017 11:00:12 PM] Participant #2 : But then everyone complained because their "gaming hardware" stopped working

[2/12/2017 11:00:21 PM] Ruben: Haha, ahh. so macro keyboards etc?

[2/12/2017 11:01:02 PM] Participant #2 : So there is probably hardware out there that does use this BUT I'm thinking they can use server-side detection to figure out that if a person is using a mixture of injected and non-injected "hardware" and they're "suspected" that they might be hacking

[2/12/2017 11:01:13 PM] Participant #2 : Yeah or like controllers of some kind..

[2/12/2017 11:01:42 PM] Ruben: What do you mean exactly by server-side detection in this context? What would it entail?

[2/12/2017 11:02:01 PM] Participant #2 : For every hardware action they send whether it was injected or not

[2/12/2017 11:02:42 PM] Participant #2 : Then on the server, they analyze the hardware actions and if they're using "injected" right before they get a headshot, then they're probably using an aimbot

[2/12/2017 11:03:16 PM] Participant #2 : Because if they were injecting 100% of the time then they're using a special mouse, otherwise it'll be non-injected 100% of the time.

[2/12/2017 11:03:34 PM] Ruben: Right, that makes sense.

[2/12/2017 11:03:37 PM] Participant #2 : It doesn't make sense that you're using mouse 1 then mouse 2 in like 1 second before a headshot

[2/12/2017 11:03:53 PM] Participant #2 : Especially when a bunch of folks reported you

[2/12/2017 11:04:14 PM] Ruben: Gotcha.

[2/12/2017 11:04:16 PM] Ruben: Last question,

[2/12/2017 11:04:21 PM] Ruben: At the very beginning you said:

[2/12/2017 11:04:26 PM] Ruben: In Windows (and OSX) they might be able to see that an application has an open handle to the game but if the application is running with escalated privileges, the anti-cheat would not be able to read the memory of that application. Furthermore, doing so would violate privacy laws in some countries.

[2/12/2017 11:05:10 PM] Ruben: The last sentence, the violation of privacy laws, where do you base this on? I ask because everywhere i go on forums i see people referencing a lawsuit that blizzard was allegedly in where a court straight up told them that scanning outside the game memory space is a privacy infringement.

[2/12/2017 11:05:21 PM] Ruben: I've scoured the internet but it just doesn't seem to exist.

[2/12/2017 11:07:00 PM] Participant #2 : I think there was a class-action lawsuit against Blizzard back in 2006-2007

[2/12/2017 11:07:11 PM] Participant #2 : And there was also the MDY vs Blizzard lawsuit.

[2/12/2017 11:07:37 PM] Participant #2 : And then there was another one in 2012.

[2/12/2017 11:07:56 PM] Ruben: Going to have to dig deeper then, hope I can find it.

[2/12/2017 11:08:09 PM] Ruben: I've seen people reference it as a class action lawsuit around that time, like you said

[2/12/2017 11:08:13 PM] Ruben: That has to be it i assume

[2/12/2017 11:08:51 PM] Participant #2 : But then again, I'm just repeating what I heard on the forums and what I've seen with VAC. I didn't really care to check whether it was true.

[2/12/2017 11:09:14 PM] Participant #2 : Only cause it kinda makes sense, if you're taking screenshots of a users computer or scanning memory of other programs, that's really bad for privacy.

[2/12/2017 11:09:49 PM] Participant #2 : And I know Europe doesn't really take kindly to companies doing that

[2/12/2017 11:10:16 PM] Ruben: You're right, and that is indeed the focus of my thesis. It is indeed at odds with privacy, especially because they're accessing your equipment.

[2/12/2017 11:10:23 PM] Ruben: The question is how far consent can go in this situation.

[2/12/2017 11:10:31 PM] Ruben: Especially if it's hidden away in a EULA somewhere

[2/12/2017 11:10:56 PM] Participant #2 : As far as I know, EULA and Privacy Policy doesn't give you the right to do that sort of scanning

[2/12/2017 11:11:48 PM] Participant #2 : And companies can't sue you for violating them. EULA is not a binding contract.

[2/12/2017 11:12:21 PM] Participant #2 : The only reason they won against MDY and I think HonorBuddy is because of copyright infringement

[2/12/2017 11:12:58 PM] Ruben: Interesting case that.

[2/12/2017 11:13:01 PM] Participant #2 : They argued that the memory produced by wow and the code is copyright and you reading it is infringing on that.

[2/12/2017 11:13:55 PM] Participant #2 : Even though some of these countries have no reverse engineering laws. even in 'murica the DMCA allows you to reverse engineer under certain conditions such as research. Canada allows all forms of reverse engineering, as far as I know.

[2/12/2017 11:14:54 PM] Participant #2 : And no Russia/Ukraine isn't 100% safe cause government might give you up, I think we saw that with kickass torrents or something where it was based in ukraine and they shut it down. Same withe MEGA lol

[2/12/2017 11:15:09 PM] Participant #2 : If you wanna do that sorta shit, China is probably one of the better places to do it in.

[2/12/2017 11:15:51 PM] Participant #2 : Oh yeah and pirate bay keeps getting hit as well

[2/12/2017 11:15:59 PM] Ruben: Interesting, reverse engineering is allowed for interoperability here.

[2/12/2017 11:16:01 PM] Ruben: As far as i know.

[2/12/2017 11:16:12 PM] Participant #2 : Yes thats one of the DMCA exceptions

[2/12/2017 11:16:32 PM] Participant #2 : Which is hilarious... my bot needs to be interoperable with the game

[2/12/2017 11:16:37 PM] Ruben: Haha

[2/12/2017 11:16:59 PM] Ruben: Out of interest, when you say; 'As far as I know, EULA and Privacy Policy doesn't give you the right to do that sort of scanning' do you base this on something specifically? Something you've read or something?

[2/12/2017 11:18:30 PM] Participant #2 : Just stuff I've read on the news and forums, etc. Privacy Policy and EULA doesn't give you the right to be a dick, essentially.

[2/12/2017 11:18:47 PM] Participant #2 : Like, they can't write "you owe us your first born" and make it true.

[2/12/2017 11:18:58 PM] Participant #2 : They can only write so much

[2/12/2017 11:19:19 PM] Ruben: Gotcha. because the more I'm reading into it, the more I'm coming to the conclusion that this particular scenario is legally possible. which is really concerning, for the reasons you've mentioned

[2/12/2017 11:19:40 PM] Participant #2 : It's definitely gray market

[2/12/2017 11:19:40 PM] Ruben: I'll know in a couple of months when everything is done .

[2/12/2017 11:19:57 PM] Ruben: man Participant #2 i can't thank you enough for this, this has been super enlightening

[2/12/2017 11:20:13 PM] Participant #2 : Glad I could help

[2/12/2017 11:20:24 PM] Participant #2 : Good luck on your thesis, I hope it goes really well

[2/12/2017 11:20:28 PM] Ruben: Do you object to being acknowledged by name or would you prefer to remain anonymous?

[2/12/2017 11:20:33 PM] Participant #2 : Maybe I can read it when you're finished :-P

[2/12/2017 11:20:54 PM] Participant #2 : Name is fine

[2/12/2017 11:21:10 PM] Ruben: I would like to reference you as an expert on the subject, could you also tell me your educational background

[2/12/2017 11:21:38 PM] Participant #2 : Bachelors of Computer Science.

[2/12/2017 11:22:23 PM] Ruben: Great, thanks. i will double-check with you before i publish anything so that you are in agreement with what I've mentioned about you or referenced you


[2/12/2017 11:22:30 PM] Participant #2 : been doing reverse engineering since about 2010 and got really involved in it back in mid 2013.

[2/12/2017 11:22:39 PM] Participant #2 : Sounds good.

[2/12/2017 11:22:52 PM] Ruben: All right man, thanks again and have a nice evening!

[2/12/2017 11:22:59 PM] Participant #2 : Yep you too!

ANNEX C(2): COMMUNICATIONS WITH PARTICIPANT #2

 Originally Posted by [Ruben Greidanus]

You've been hired by the government data protection agency to carry out audits on online gaming companies (let's say, the 'average' game company, so not Blizzard, maybe something like Funcom). They want you to assess the state of their anti-cheat strategy with regards to user privacy. The government agency wants you to find out:

- How invasive the system is. You wouldn't have to know all the exact details, just a general impression on how far the techniques go. For example, you find out all they do is scan the game memory space for blacklisted code. You'll report back it's not too invasive. Or, you find that they actively try to take screenshots of the users desktop - you report back it's quite invasive.*
- Whether their detection methods are adequately designed. For example, if it checks window titles, does it use hash-validation (or other pseudonymization techniques) so that it doesn't come into actual context with the actual title string itself?*
- Whether they're over relying on client-side anti-cheat. So: are they using it for things that could easily be done with server-side detection, for example?*

Imagine this has been your job for over a year, and you constantly audit companies like this. You've had quite a bit of time to further educate yourself on the subject and have built your own pool of knowledge and expertise. The programmers at these companies cooperate fully with any request you make. They would know in advance you were coming, and could prepare accordingly in order to speed up the process. You could send them instructions in advance.

How long do you estimate it would take you to assess all of the above and report on it, on average? I don't expect specifics obviously, just an estimation.

So a lot of companies here in Canada, including mine, apply for [SR&ED](#) grants from the government. Although I don't know exactly how much paperwork and communication happens in the background, I do know that an auditor comes by every few months to interview our developers about the research they've been doing. We also supply them with design documents and data about our progress over time. I would imagine it's no different here.

Now, any competent security firm who is hired to analyze these companies would likely already have the necessary paperwork and checklists to ensure the game companies' compliance with the countries' privacy laws. I would also imagine that the security firm has it's own set of tools for analyzing the game clients, akin to Apple's App Store or government car emissions tests. This would certainly speed up the processes immensely.

Now, prior to interviewing the developers or running any tests, the security firm would request and analyze design documents about the anti-cheat system to assess how best to verify their compliance. This might take several weeks depending on complexity. After that, the firm would schedule an interview with the anti-cheat team and ask tailored questions about their system, depending on the answers, follow-up interviews may be scheduled. But let's say a week to schedule and conduct a single interview. Finally the security firm would then run their own tools on the client to verify its implementation. This might take another several weeks depending on complexity and whether a custom client is required.

Overall, I don't imagine it taking more than a month on average to complete per company. And multiple companies would get audited at the same time. A lot of it has to do with how much information is available up front. If the game company has competent developers that know their system inside-out and can convince the security firm that they know what they're doing, then the audit is completed very quickly. If no one knows that they're doing, then honestly the sky's the limit.

I hope this answers your question. Good luck on your paper and let me know if you have any follow-up questions.