MEDIÁLNÍ STUDIA
MEDIA STUDIES
JOURNAL FOR CRITICAL MEDIA INQUIRY

Who watches the watch dogs?
How Watch Dogs 2 represents hacker culture and hacktivism
John J. Fennimore

To cite this article:
Fennimore, J. J. (2020). Who watches the watch dogs? How Watch Dogs 2 represents hacker culture and hacktivism. *Mediální studia*, 15(1), 43-61.

ISSN 2464-4846
Journal website: https://www.medialnistudia.fsv.cuni.cz/

1/2021

WHO WATCHES THE WATCH DOGS? HOW WATCH DOGS 2 REPRESENTS HACKER CULTURE AND HACKTIVISM

JOHN J. FENNIMORE
North Carolina State University

ABSTRACT

In Watch Dogs 2, players team up with a collective of hackers to expose the dangers of the city-wide online infrastructure and the company behind it. Hacktivists in the physical world subvert computer systems to protect the public's digital privacy and agency against private interests. While hacktivists often disregard the law, they hack in disruptive yet nonviolent ways to encourage social changes. While hacking is a common gameplay mechanic in many mainstream games, there is relatively little research investigating games about hacking. This textual analysis examines how Watch Dogs 2 succeeds and fails in representing hacktivism. Watch Dogs 2 lovingly embraces the attitudes and values of hacktivists. Through its simulation of hacking, the game helps players understand what makes hacking so enthralling. However, the ethical argument the game makes for hacktivism is threatened by story and gameplay decisions made to keep the game appealing to the audiences of the game's publisher, Ubisoft.
Keywords: *Watch Dogs 2* ▪ Ubisoft ▪ representation ▪ hacker ▪ hacktivism ▪ video games

1. INTRODUCTION

In July 2020, weeks after news broke of how game publisher Ubisoft mishandled dozens of employee claims of sexual misconduct (Schreier, 2020), the publisher announced that anyone who logs into their Uplay accounts during Ubisoft Forward – a livestream announcing upcoming games from the publisher (which would not address the allegations as per another announcement from Ubisoft (Bankhurst, 2020)) – would receive a free copy of *Watch Dogs 2* on PC (Sitzes & Petite, 2020). In the context of the sexual misconduct scandal at Ubisoft, the giveaway might be seen as a way for Ubisoft to help keep its audience on its side.

Ubisoft's *Watch Dogs* series of games is well known for embracing the concept of hacktivism and the culture surrounding it. The official website for *Watch Dogs 2* informs players that they can "ignite the rebel in you and break the rules – for the

lulz [sic], for what's right, and most importantly, because you can" (Ubisoft, 2016). A player teams up with the San Francisco chapter of DedSec, a worldwide collective of hackers, to expose the dangers of the city-wide online infrastructure and the company behind it. The plucky group of young heroes create their very own social movement based on hacktivism – the promotion of a political agenda or social change through technology (Manion & Goodrum, 2000) – as they accrue followers to their cause through social media to strengthen their abilities and influence. The group organizes demonstrations against organizations and corporations who exploit people's data for their own financial and political gain. However, DedSec go beyond traditional activism to break into offices and find evidence of suspect behavior.

Even if a game is not primarily about hacking, users have likely played a mainstream game with a hacking mechanic from *Bioshock* to *Deus Ex: Human Revolution*. Despite the popularity of hacking as a game mechanic in many popular games, there is relatively little research investigating games about hacking. Game studies has mostly investigated how users hack or modify video games (Boluk & Lemieux, 2017; Murphy, 2013), including how hacking a game reveals or creates new meanings about games as intellectual property (Kretzschmar & Stanfill, 2019; Postigo, 2008) and how hacking changes the way people play games (Newman, 2018; Zhao & Zhang, 2019). This study aims to expand the scope of academic research not only on how hacker culture is represented in mainstream media but on how a video game's gameplay can complicate or, in the case of *Watch Dogs 2*, threaten to ruin the message of its story.

The article begins with an overview of the relevant literature on hacktivism and hacker culture to establish the core definitions. The article then goes into a textual analysis of *Watch Dogs 2*, with a focus on how accurately the game represents the definitions and core values of hacker culture and hacktivism through both the story and the gameplay. The scope of this article is limited to the main story missions, the side missions, and the cutscenes between each story mission. It will not incorporate the missions included in the game's paid downloadable content.[1] I argue that *Watch Dogs 2* lovingly embraces the attitudes, ethics, and values of hacktivists. Through its simulation of hacking, the game helps players understand what makes hacking so enthralling. However, its portrayal of hacktivism is threatened by story and gameplay decisions made to keep the game appealing to Ubisoft's audiences.

2. LITERATURE REVIEW

2.1. Definitions: Hacking, hacker, and hacktivism

As Powell (2016) notes, previous research on hacking was largely concerned with

1 *Watch Dogs 2* has a season pass offering new missions, multiplayer modes, items, and enemy types. Not every player buys season passes, so their understanding of the story is limited to the base game. Thus, incorporating the missions from the season pass would not add much to the analysis.

how it illuminates new ways of both engaging with and changing the function of machines, intellectual property, and materials. Many have also attempted to explain the general culture and values of hackers. Pawlicka, Choraś, and Pawlicki (2021) note that defining the hacker is difficult because the backgrounds and motivations of hackers are diverse despite the mainstream representation of hackers as anti-social basement dwellers who crack computer security in the name of cybercrime.

While hacking can appear in many different forms – from the iconic image of a hacker soldering a circuit board to an internet troll creating bots to spread misinformation on social media (Pawlicka, Choraś, & Pawlicki, 2021) – hacking can be defined as "critical, creative, reflective and subversive use of technology that allows creating new meanings," (Kubitschko, 2015, p. 83). Comparing the work of hackers to the work of creative artists, Nikitina (2012) calls hackers' work procedures "reverse creativity." Hackers start with an already created project and work backwards from the creator's thought process to find flaws that they can exploit. According to Powell (2016), hacking can represent a democratization of technical or scientific knowledge while hackers establish their own authority rooted in the imagination and expertise consolidated through participation. The activity of hacking is inherently political. "DIY and hacking culture operate by undermining and appropriating systems and structures through material practice," (Powell, 2016, p. 613). Hackers and the computer industry evolve together (Söderberg & Maxigas, 2021), and thus a key part of hacker culture is the symbiotic yet antagonistic relationship between hackers and the industry. "Applied to our context of inquiry, hackers are conditioned by the technical infrastructure upon which they draw, as well as the labor demand for their services," (Söderberg & Maxigas, 2021, p. 47).

Hacktivism falls under the definition of electronic civil disobedience, as it "does not condone violent or destructive acts against its enemies, focusing instead on nonviolent means to expose wrongs, raise awareness, and prohibit the implementation of perceived unethical laws by individuals, organizations, corporations, or governments," (Manion & Goodrum, 2000, p. 14). This is different from electronic activism which simply uses the internet to share information, coordinate action, and lobby policy makers (Manion & Goodrum, 2000). The goal of hacktivism is to create a disruption in technology and promote activism (Manion & Goodrum, 2000). Other criteria include 1) no damage to people or property, 2) no financial gains, 3) actions grounded in ethical motivations, and 4) accountability for actions (Manion & Goodrum, 2000). Hacktivism is also different from cyberterrorism, damaging hacks targeting governments and societies in order to intimidate them into adopting certain political ideologies (Denning, 2006).

Examples of hacktivism can be found in video games. In 2018, a user hacked the online player ranking system of the Nintendo game *Splatoon 2* and wrote the message "please add anti-cheat" across the leaderboard (Clark, 2018). The user hacked *Splatoon 2* because the game was rife with cheaters while Nintendo was doing nothing about them (Clark, 2018). The act is an example of hacktivism because it was

a disruptive yet nondestructive hack that called attention to an issue. Another notable example of players disrupting a video game is the Running of the Gnomes event in *World of Warcraft*, where players recreate the offline breast cancer charity event, Race for the Cure, by playing as pink-haired gnomes in pink clothing and racing though the virtual world. Collister (2017) argues that the event reflects hacktivism even though its organizers do not frame the event as hacktivism. The event is disruptive rather than destructive to the game world, though the game's server can crash due to the sheer volume of player participation. It also raises awareness of an issue as the game's chat boxes are flooded with messages about breast cancer. While no one alters the game's code during the event, the event could be seen as a hack because it subverts the intended role-playing gameplay of *World of Warcraft* (Collister, 2017).

2.2. The values and ethics of hacker culture

Coleman's ethnography of the San Francisco hacking scene discusses how hacking is characterized by "a confluence of constant occupational disappointments and personal/collective joys," (Coleman, 2013, p. 11). As a performative act taking the forms of inside jokes or humorous hacks, humor in the hacker world not only expresses the joy of hacking but also represents the hacker's definition of creativity and individuality.

"This expression of wit solidifies the meaning of archetypal hacker selves: self-determined and rational individuals who use their well-developed faculties of discrimination and perception to understand the 'formal' world – technical or not – around them with such perspicuity that they can intervene virtuously within this logical system either for the sake of play, pedagogy, or technological innovation. In short, they have playfully defiant attitudes, which they apply to almost any system in order to repurpose it," (Coleman, 2013, p. 7).

On the contrary, hacking is often a frustrating activity as hackers navigate and tinker through software and technology. Hacking demands that users both tolerate frustration and deeply engage with the activity (Coleman, 2013). As hackers overcome baffling problems in technology, they can enter a state of eudaemonia or the feeling of joy stemming from the self-directed realization of skills, goals, and talents (Coleman, 2013). Eudaemonia is central to hackers' sense of accomplishment and pride. Hackers feel gratified not only working with the functions and limits of technology but creating new functionalities that the original creators do not intend (Coleman, 2013).

Hackers derive pleasure in outwitting constraints both collectively and individually. As hackers copied lines of code from friends and modified their software early in their hacker lives, they learned that they were bound to their peers through coproduction although there is also a competitive element to the interaction (Coleman, 2013). Hackers emphasize a culture of meritocracy and individuality in the way they value unique and clever hacks as well as their performative humor (Coleman, 2013). At the same time, however, much of hacker production is collective, subverting the values of individuality. Söderberg & Maxigas (2021) suggest that passing down expertise and

shared cultural values to new generations of hackers is key to what they call the functional autonomy of hackers, which enables hackers to illuminate new ways of critically thinking about predominant technological designs and to create alternative pathways.

Hackers can be categorized by their expertise (what they know), values (what they are), actions (what they do), and tools (what they have) (Jaquet-Chiffelle & Loi, 2020). Their moral principles define the legal and/or ethical limits that they respect while trying to reach their objectives. According to Coleman (2013), all hackers share a relation to legality despite differences in ethical motivations and values; their actions reveal legal grey areas and emerging legal meanings. "Hackers provide less of a unitary and distinguishable ethical position and more of a mosaic of interconnected, but at times divergent, ethical principles," (Coleman, 2013, p. 19).

The most common categories of hackers include white hats, black hats, grey hats, ethical hackers, script kiddies, true hackers, and hacktivists.[2] White hats are skilled programmers who search for vulnerabilities in cyber security to defend information and to prevent attacks from malicious hackers. Ethical hackers are white hats hired to hack into a client's system under a set of formal rules to find and to patch vulnerabilities.[3] Black hats are skilled programmers who find and exploit vulnerabilities in cyber security for personal financial gain and other malicious intentions with no regard to the violation of laws or ethics.[4] Grey hats are skilled programmers who search for weaknesses in computer security for fun, for a challenge, for peer recognition, or for the improvement of security. Grey hats' intentions may not usually be malicious, but their actions might not necessarily respect applicable laws.[5] True hackers, originating in the hackers from west coast counterculture in the 1960s (Jaquet-Chiffelle & Loi, 2020; Levy, 2010; Tuner, 2006), believe in the positive impact of computers and information access and hack only for personal fun and challenge while respecting the law. Script kiddies are inexperienced hackers who use tools and code developed by more experienced hackers. Hacktivists are skilled programmers who exploit weaknesses in computer systems not for personal gain but to further a political cause, opinion, or ideology. While the actions of a hacktivists are ethically motivated, hacktivists do not usually respect laws. Hacktivists are generally left-wing, anti-capitalist, and anti-corporate idealists who hack to expose the secrets of large corporations or governments and to encourage social and political changes (Pawlicka, Choraś, & Pawlicki, 2021). Sometimes they leak classified documents in

2 The following definitions come from Jaquet-Chiffelle and Loi (2020).

3 Pen testers are white hats who specialize in penetration tests, or the simulation of an attack on a computer system. According to Jaquet-Chiffelle and Loi (2020), all pen testers are white hats but not all white hats are pen testers.

4 All black hats are cyber criminals according to Jaquet-Chiffelle and Loi (2020), but not all cyber criminals are black hats as they may not have the expertise all black hats have (they may copy hacks developed by black hats). Crackers, defined by Jaquet-Chiffelle and Loi (2020), are black or grey hats who specifically break into computer systems without permission. Many hackers use the term crackers to differentiate themselves from cyber criminals (Ali Saifudeen, 2021; Coleman, 2013; Jaquet-Chiffelle & Loi, 2020).

5 Many grey hats follow their own moral principles that differ from the law or from other hackers' ethics.

the name of free speech or send DDoS attacks on corporate websites to protest the actions of the corporation. Hacktivists especially crave publicity and share their actions on social media (Mansfield-Devine, 2011).

Hackers deconstruct technology while building and maintaining alternative ones. As Söderberg and Maxigas (2021) argue, "embedded in the word 'hacking,' and key to the hacker identity, is the promise that freedom can be realized through the repurposing of tools and by routing around constraints and regulations," (p. 43). Hacktivism as a form of political engagement includes digital direct action serving a watchdog function. Hackers not only share their knowledge with citizens through public gatherings and through mainstream media coverage but also advise politicians and legislators. According to Kubitschko (2015), hackers' activities spread awareness and knowledge to enable others' engagement. Many hackers are privacy advocates who are concerned with transparency in government, communication as a human right, free access to communication and information infrastructures, and developing alternative methods of communication for citizens that are more anonymous, secure, and safe from state and corporate interests (Kubitschko, 2015). Anonymous communication is especially important because anonymity is often the catalyst for whistleblowing (Kubitschko, 2015).

> "Understanding how something works is a prerequisite for judging its significance and ramifications. The technical expertise of hackers has allowed them to intervene in politics in more consequential ways than is the case with the 'prefigurative politics' of many social movements. The paths taken by hackers in terms of technology choice have not only demonstrated the possibility of an alternative, but have on many occasions forced the computer industry to follow suit," (Söderberg & Maxigas, 2021, p. 48).

Hackers can be divided by their actions, expertise, tools, and values, but are united by their ability to alter and undermine computer systems to shed light on new ethical and legal meanings about how they function. Hacktivists work to push political ideologies by subverting computer systems and creating a disruption. The actions of Hacktivists may not be legal but are ethically motivated. Hackers also take accountability for their actions, never hack to inflict violence, and never hack for personal financial gain. This understanding of the multifaceted cultures and ethics of hacker culture will direct the textual analysis of *Watch Dogs 2* and inform the article's investigation of how the game represents the definitions, values, and ethics of hacktivism through its story and gameplay.

3. METHODS

The textual analysis will use Bogost's theory of procedural rhetoric as a frame of reference (Bogost, 2007). Procedural rhetoric is "the practice of persuading through

processes in general and computational processes in particular... [and] a technique for making arguments with computational systems and for unpacking computational arguments others have created," (2007, p. 3). Game designers make claims about phenomena in the physical world by modeling them through digital simulation. The decisions game designers make in crafting the simulation changes what the simulation tells the audience.

> "We must recognize the persuasive and expressive power of procedurality. Processes influence us. They seed changes in our attitudes, which in turn, and over time, change our culture. As players of videogames... we should recognize procedural rhetoric as a new way to interrogate our world, to comment on it, to disrupt and challenge it. As creators and players of videogames, we must be conscious of the procedural claims we make, why we make them, and what kind of social fabric we hope to cultivate through the processes we unleash on the world... the logics that drive our games make claims about who we are, how our world functions, and what we want it to become" (Bogost, 2007, p. 340).

Grounded in the overview of the relevant literature, the textual analysis examines how *Watch Dogs* 2 succeeds and fails in representing hacktivism. The analysis concentrates primarily on the cutscenes that play before, during, and after the 15 main story missions as well as the conversations that occur between the characters during the gameplay of the story missions. I also considered what the player does within the missions, what actions they can perform within the virtual world, and how the game mechanics govern their actions into the analysis. As Bogost and others (e.g., Malaby, 2007) argue, the design of a game shapes the messages and themes players interpret from the experience of the game, and thus the gameplay has just as much bearing on the analysis as the story. I also included the gameplay and story content of side missions, though the side missions were not the primary focus of the analysis. I analyzed and evaluated the scenes and gameplay based on the criteria of hacktivism: the actions of the characters promote political ideologies, actions are ethically motivated regardless of legality, actions are disruptive yet nonviolent, actions do not lead to financial gain, and the hackers take accountability for their actions.

4. ANALYSIS

4.1. Representation of hacker culture

Watch Dogs 2 involves a city-wide operating system known as ctOS 2.0, created by Blume Corporation to secure safer and more efficient metropolises according to the game's official website (Ubisoft, 2016). However, many believe that corporations are

using ctOS to monitor and manipulate citizens for profit. You play as Marcus Holloway, who was wrongfully flagged by predictive algorithms as the primary suspect of a high-tech robbery. Under the alias "Retr0," he leaked incriminating documents on the predictive algorithm and then joined DedSec after he snuck into Blume's offices to erase his criminal profile (Ubisoft, 2016). To take down Blume and ctOS, DedSec need to accrue followers to their cause by performing public stunts and exposing dark secrets within Silicon Valley. This not only separates them "from the trolls" as one DedSec member said, but also strengthens their technological capabilities (Ubisoft, 2016). By signing up in the DedSec app, followers can pledge to donate the processing power of their devices to DedSec. The game's progression system for hacking abilities reflects this story element. Similar to role-playing games where players earn experience points until they level up and increase their stats, players in *Watch Dogs 2* gain followers by completing missions and doing other activities until they reach a certain threshold and earn points usable to learn new hacking skills like shutting down security cameras or hacking cars to control them remotely.

The goal of growing followers is in line with the hacktivist ethos. Contemporary social movements take advantage of social media and other digital tools to quickly amass tons of protesters under a common cause (Tufekci, 2017). Hacktivists in the physical world aim to share their information with as many people as possible. Hacktivists want people to know how corporations and governments exploit their data because such knowledge gives people the power to try and take back control. Also, social movements can use digital platforms to further their goals and craft and amplify their own narrative (Tufekci, 2017). DedSec do this throughout the game; they share the incriminating evidence they find through videos stylized with their unique visual artistry inspired by videos from the real-life hacker collective Anonymous. An audio log in Blume's headquarters says that DedSec put their company "firmly into their warped perception of 'bad guy' territory," but DedSec's narrative of the dangers of big data is backed up by the cold facts they unearth (Ubisoft, 2016).

The cooperative element of hacking is also apparent in the gameplay. The leaderless nature of DedSec allows everyone an equal chance to contribute. The success of DedSec also hinges on the support they can grow from followers, not only in how the player's abilities grow but in how other DedSec members occasionally provide intel before a mission starts. Part of the reason the group gets back on track after losing morale in the middle of the story is by attending a hacker festival in the desert. The competition that they win helps reestablish their group solidarity, an important aspect of real-life hacker conventions (Coleman, 2013). The game's integration of online multiplayer further reinforces the collaborative spirit of hacking. If players are open to online play, players can occasionally encounter other players in their game and choose to join them on exclusive co-op missions (Ubisoft, 2016).

However, the competitive aspect of hacking is also apparent in the game. The hackers of DedSec have their own unique personalities and sense of humor which occasionally clash with one another. This reflects the concept of hackers using wit

and humor to distinguish themselves from one another (Coleman, 2013). DedSec are in opposition to a rival hacking group known as Prime_Eight, who sell and exploit data to anyone with money including Blume and even terrorists. DedSec's opposition to Prime_Eight is also accurate in showing how people in hacker culture tend to distance themselves from crackers (Ali Saifudeen, 2021; Coleman, 2013; Jaquet-Chiffelle & Loi, 2020). The multiplayer mode reinforces the competitive aspect of hacker culture in addition to its cooperative one. A player can invade another player's game and try to hack it while the target tries to hunt the invader down.

The gameplay, through simulation, symbolizes both the joys and frustrations inherent to hacking. Most missions involve game players sneaking around a restricted area filled with guards who would shoot the player on sight. Players must use their hacking abilities and observation skills to evade the guards and to complete the objective. Players can use their smartphone to hack all kinds of things for different effects. They can make electric gauges and panels shock nearby guards or just cause a distraction (see Figure 1). They can use remote-controlled gadgets to scan for guards and even distract them with sounds. *Watch Dogs 2* is as much a puzzle game as it is an action game. Not everything goes as planned, so the player must deal with those frustrations accordingly.

Figure 1: The player about to shock a guard by hacking an electrical panel. Image source: Watch Dogs 2 (Ubisoft Montreal), image captured and modified by the author.

Similar to the process of hacking, the core gameplay of *Watch Dogs 2* invites players to subvert and repurpose the design of the level to complete objectives (Ali Saifudeen, 2021; Powell, 2016; Söderberg & Maxigas, 2021). Players begin by surveying the area and then deconstruct it down to its individual interactive elements and obstacles.

Players then figure out flaws in the system. When the player leaves the area with the task complete, satisfaction rushes through their body at a job well done. It embodies the idea of hacking as "reverse creativity" (Nikitina, 2012) where players work backwards from an already completed system to find flaws and exploit them. The game simulates hacking by reflecting its subversive and satisfying nature.

The hacktivists of *Watch Dogs 2* look, act, and think like real life hacktivists. They value freedom of access and the right to privacy while fighting against anyone who uses technology to exploit the public. The way they fight is by informing the public about how companies and governments exploit the public's data. Sharing information is DedSec's way of helping people take back the power. As the number of DedSec's followers grows, so does DedSec's ability to encourage social changes. Increasing the number of followers improves not only players' hacking abilities but also the strength of the movement overall. The gameplay immerses players in the cooperative and competitive aspects of hacker culture keeping hackers together as well as the subversive joy of hacking itself. *Watch Dogs 2* helps players understand the potential impact of hacktivism and why it is so compelling to perform.

4.2. Representation of hacker ethics and values

Like hackers of the offline world, the hackers of DedSec embrace liberal ideals of free speech, access, transparency, equal opportunity, and publicity. One of the earliest cutscenes in the game talks about how tech companies watch every move of their customers and craft a digital profile on each customer "to be bought, sold, or stolen in an instant," (Ubisoft, 2016). Most of the hackers, including Marcus, who form the core group of DedSec in San Francisco were burned by the effects of big data, and now all of them fight so that big data cannot abuse anyone else. All the members of DedSec share the playfully defiant attitudes embodied by many hackers (Coleman, 2013). Their attitudes come not only from their sense of humor and technological expertise, but from their capacity to perceive the true intentions of big data and apply their expertise in stopping the intentions. "I say we tear down the fucking wall, show everyone what Blume's been up to, man. Show the world that their personal data is being used to rob them of their fucking freedoms," Marcus says (Ubisoft, 2016). The group also practices what they preach; the DedSec app is transparent about the way it collects processing power while never collecting personal data.

Through the actions of DedSec, the game attempts to make an ethical argument in favor of hacktivism. DedSec expose wrongs, raise awareness, and prevent unethical laws and practices from being established, which is a key trait of electronic civil disobedience (Manion & Goodrum, 2000). Over the course of the story, DedSec reveal the criminal intentions of a religious cult and expose Blume and a security firm's plan to put ctOS functionality into armed robots and to use the robots against civilians. DedSec also expose Blume and a social media company's plan to manipulate users' social feeds and to rig election machines for a political puppet. At the end of

the game, DedSec reveal that Blume's CTO, Dušan Nemec, was using his access to all the data that Blume collected from ctOS to create a program that could manipulate stock markets, other tech companies, and the public. DedSec also take accountability for their actions. In fact, during the mission called "Hack Teh World [sic]," Marcus leaves the symbol of DedSec drawn in red lights on the servers of Blume's Dublin office after downloading all their data (Ubisoft, 2016).

While DedSec's actions, namely breaking and entering as well as stealing and leaking confidential information, are illegal, *Watch Dogs* 2 attempts to ethically argue that the actions are justified. According to Jaquet-Chiffelle and Loi (2020), one can make an argument that a choice was the most (or even only) ethical option if they take the viewpoints of everyone involved into account. Sometimes the most ethical option is not legal. A white hat by principle does not share the secrets of a client when they break into their systems to find vulnerabilities. However, if a white hat discovers that the client is committing serious crimes, then breaching trust and sharing the discovery with law enforcement would be an ethically optimal action (Jaquet-Chiffelle & Loi, 2020).

> "If their ethical values conflict with those at a business level their ethical evaluation of the situation will depend on the prioritization of the values. A strong personal ethical value or a well-established important societal value might prevail on any other business-related value and lead to breaking the code of conduct. This is in particular true if the ethical hacker unveils critical non-ethical behaviors within the company. In this case, the evaluation of whether the hacker is ethical will be significantly more complex (Jaquet-Chiffelle & Loi, 2020, p. 201).

Marcus and the rest of DedSec are not white hats of course; they are hacktivists. We can view the actions of hacktivists as unethical as it works against the interests of the people or organizations they target. However, if the actions lead to the targets being held accountable for their unethical behavior and prevents them from continuing their behavior, then we can view the hacktivist as acting ethically (Jaquet-Chiffelle & Loi, 2020). If privacy ought to be a universal right, then breaking into a system and leaking the secrets of a corporation to the public would be a violation of that right and therefore unethical. However, if a company is secretly doing unethical things, then one could make the argument that exposing the secrets to the world would be ethical. A key moment in *Watch Dogs* 2 where Dušan confronts Marcus especially explores the dynamics of ethics:

> *Dušan: "Guess what, Marcus! GUESS WHAT! The people want to be told who is good and who is bad. They don't care how it works, only that it does."*
> *Marcus: "But it doesn't fucking work!"*

> *Dušan: "A few fucking civilian casualties is the cost you have to pay for the betterment of the world. You're fighting a war no one gives a shit about."*

Dušan argues that it does not matter what Blume does with ctOS so long as the public is satisfied with ctOS making their lives more convenient. The loss of life from flaws in ctOS is a small cost to pay as Blume improves ctOS so it can better help people around the world. The ethics of DedSec's actions are contingent on privacy being a universally ethical value as the societal value would prevail over Blume's business-related values. Dušan argues that because people do not care about how their data is being used, DedSec do not have an ethical leg to stand on.

However, DedSec work to raise awareness about the ways that companies violate the privacy of the people who use their services, helping to drive the conversation about it and making digital privacy a societal value. The increase in awareness is evidenced by how the follower account rises when players complete both story and side missions; more and more people are embracing DedSec's message. By the end of the game, the movement grows so much that even Blume starts to notice how large, loud, and stubborn public support of DedSec are according to an audio log in the final mission (Ubisoft, 2016). The growing public concern helps DedSec make an ethical case in exposing Blume and Dušan, even if their actions involve breaking into offices and stealing data. *Watch Dogs 2* shows that when the public concern for privacy outweighs the profit motivations of tech companies, the actions of hacktivism in holding tech companies accountable are ethical.

The game also makes an argument through the story that hacktivists can break through the limits that restrict traditional systems from holding companies accountable. During a story mission where players are tasked with exposing a criminal organization masquerading as a religious cult known as New Dawn, Marcus meets with a councilwoman known as Miranda Comay. She has been trying to expose New Dawn for years, but her actions are limited because she is a councilwoman as she tells Marcus. However, Marcus can expose New Dawn on her behalf because of his status outside of the law (Ubisoft, 2016). This reflects the way that hacktivists can inform government bodies to bring about change; hacktivists have a different set of ethical limits that define their actions compared to government and thus can act in different ways to hold people accountable.

While DedSec's actions are ethically motivated, DedSec do not follow the other criteria of electronic civil disobedience: no financial gain, no damage to people or property, and non-violence. Money is a significant part of the progression of the game as players can buy new weapons, cars, drones, paint jobs, and clothing. Players can hack the bank accounts of non-player characters on the street and take their money, pick up money from guards they knock out, and even rob cars. This runs counter to the ethical value of hacktivists doing their work to advance political change but not to pursue personal financial gain. Players can win races if they want to earn money without hacking or hurting people (Ubisoft, 2016). However, the more money players

receive, the faster they can buy all the cool stuff they want; the game encourages players to find money by any means.

Marcus, and by extension the player controlling him, can complete his missions without any violence by sneaking though the environment undetected. However, not only does the non-violent gameplay require more skills than the average player, but the game at best does not encourage players to go the non-violent route and at worst actively dissuades them. *Watch Dogs 2* has a total of 32 weapons, five of which are non-lethal. All these weapons can be bought and crafted via a 3D printer in the hackerspaces in the game world (see Figure 2). At launch, the game had only two non-lethal weapons: a taser gun and a launcher that shoots stun grenades. Ubisoft added three more non-lethal weapons to the game via updates after launch, two of which are locked behind the "No Compromise" paid DLC (Ubisoft, 2016). While these weapons are non-lethal, it does not make the weapons non-violent. The non-lethal weapons are not as effective as the lethal ones. Players have much better odds completing missions with more potent (and permanent) weaponry. Lethal weapons are also more effective in neutralizing rival hackers in a competitive multiplayer mode. Not only does the gunplay undermine the ethics of DedSec's actions, but it hurts the spirit of hacking as players can just delete guards from the area instead of working around them.

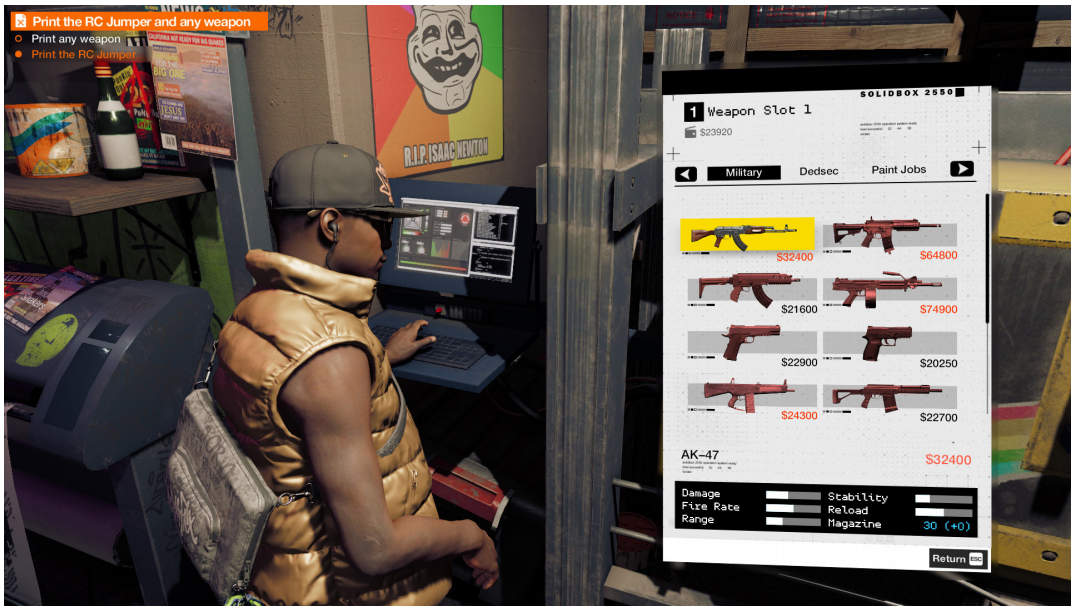

Figure 2: The player can select several lethal weapons to make with the 3D printer in DedSec's hackerspace. Image source: Watch Dogs 2 (Ubisoft Montreal), image captured and modified by the author.

While most of the violence is avoidable, there are some unavoidable story-related moments that go against DedSec's values. Some side missions involve invading people's privacy; Marcus hacks into people's cameras and live streams the footage of

himself pulling pranks on them to his followers. Invading the privacy of people like Dušan follows DedSec's imperative of holding people who violate other people's privacy accountable for their actions. However, when it is performed just for a laugh or to scare someone straight like in some of the side missions it goes against that imperative. DedSec's most destructive act occurs during "Hack Teh World." During the mission, DedSec put a virus on a satellite before it is launched into space. Once the satellite is in space, DedSec hack different places around the world, which includes disabling a power plant and compromising a server farm. During the mission called "Robot Wars," Marcus takes control of a drone to destroy the research facility it is housed in (Ubisoft, 2016). The actions in these two missions could be examples of cyberterrorism (Denning, 2006).

Moreover, the game does not properly recognize unethical behaviors. There is no morality or reputation system unlike the previous *Watch Dogs*. The story itself barely engages with the ramifications of DedSec's more destructive acts while only briefly reminding players that the acts are probably illegal. The few times Marcus finds himself on a criminal watch list are quickly resolved. At one point after celebrating a victory, Marcus drunkenly refers to DedSec as the "baddest motherfucking hacking, coding, stealing – we don't tell the cops I said that," (Ubisoft, 2016). In the latter half of the game, a news report mentions that the people support DedSec's efforts "if not their methods," (Ubisoft, 2016). In fact, all these actions are seen as the way to create social changes. It is these actions that put Dušan in prison. The game for the most part uncritically views DedSec's actions leading up to the arrest of Dušan as ethically acceptable. The game ignores DedSec's violent actions when attempting to argue in favor of hacktivism.

5. DISCUSSION

What defines all hackers is their ability to alter technology systems and create new meanings. For example, a white hat can show a client how a seemingly impenetrable security system can be circumvented. Whereas the process of reverse engineering a system can be frustrating, it only makes the success of overcoming the system more satisfying. Hackers are bound not only to their peers through both cooperation and competition but also to the tech companies that develop the infrastructure they work with and aim to circumvent. What makes each hacker different is their actions, expertise, legality, and ethics. This defines what hackers do and the limits of their actions.

Hacktivists believe in the transformative power of technology but also recognize how it can be abused to harm people for personal gain. They believe in the value of privacy, access, and freedom of information. Their work lies in modifying computer systems in disruptive yet nonviolent ways to make statements about how the systems work to rally social changes. Not only do they attempt to change technological infrastructure and how it is run, but they also create and maintain alternative

technology that helps preserves people's freedom and free access to technology. The knowledge and new meanings that they share potentially empowers not only other hacktivists but all citizens to take back control of their lives. As most of our lives are run by digital technology, subverting technology has the potential to subvert and change how society works.

DedSec exposing and stopping the abuses of tech companies and government entities falls in line with the hacktivist values of free speech, access, privacy, and agency. While many of DedSec's actions are illegal, DedSec make a case for the ethics of their actions because they lead to positive social and political changes. DedSec raise awareness to build up their individual and collective hacker values into societal ones. By revealing hidden truths such as how people's data are being used for private interests, DedSec justify their unlawful actions. However, the ethical justifications of their actions are undermined both because the ends do not justify the means (i.e. invading the privacy of targets just to prank them) and because the means do not justify the ends (i.e. killing guards, destroying property, and stealing money while exposing secrets). The game barely supports more ethical actions such as completing objectives without violence and outright forces the player to commit unethical actions. *Watch Dogs 2* fails to back up the representation of hacktivism's ability to encourage social changes by failing to commit to the criteria of nonviolence and no financial gain.

Watch Dogs 2 immerses players in the mindset of a hacktivist and helps players understand why hacktivists do the things they do. Its characters and stories embrace the playfully defiant attitudes of hacker culture and the anti-corporate, pro-freedom mindset of hacktivists. The gameplay replicates both the joys and frustrations of the creative process of hacking, not to mention its cooperative and competitive aspects. Players come to understand what makes hacking so exciting and fulfilling. The game has many moments that build its case for both the ethical foundation and the importance of hacktivism even if hacktivist actions are unlawful. However, the game does not commit to hacktivism's criteria that hacks should be made without violence against people or property and should not be made for financial gain. The destructive hacks seen in the game do not represent the actions of hacktivists in the physical world. Like all hackers, hacktivists are limited in what they can do by the values that they choose to follow. If the game was following all the principles of hacktivism, then the game should not allow the player to commit violent acts or acts made for financial gain.

6. CONCLUSION

Watch Dogs 2 argues that hackers are essentially the Robin Hood of today. They steal from the rich and powerful and give to the poor. Instead of stealing money (though DedSec can steal from both the rich and the poor), they steal information and data to prevent the rich and powerful from abusing and exploiting the poor and

vulnerable. This requires illegal operations. However, because hacktivists stop abuse and encourage social changes, they could make the argument that their actions are ethically optimal. As the unknown woman in one of the early cutscenes of the game says, "whistleblowers, activists, and hackers have drawn their battle lines, putting the establishment on watch. But are they threats themselves, or have they become freedom's last line of defense?" (Ubisoft, 2016). As the game posits, hackers like the ones in DedSec are the latter.

The game embraces the hacktivist ideals of freedom of information, privacy, and agency and demonstrates how tech companies and governments abuse the power of technology for their own gain. However, whereas the developers of *Watch Dogs 2* are making a rhetorical argument through the gameplay about the power of hacktivism in changing society for the better, they are ruining their own argument by including the option of violence and unavoidable story moments that go against the ethical values of its characters. *Watch Dogs* is Ubisoft's take on Rockstar Games' incredibly successful *Grand Theft Auto* franchise, and thus replicates much of *Grand Theft Auto*'s gameplay of looting and shooting. The crime simulation that defines *Grand Theft Auto* may have been fine for the first *Watch Dogs* game where the tone was moody. However, it does not fit with the quirky, revolutionary tone of *Watch Dogs 2*. In fact, it threatens the game's ethical argument for hacktivism.

The developers do not completely discount the value of peaceful protest and electronic civil disobedience. If they did, Dušan would likely have been killed in some over-the-top boss battle instead of going to prison. However, the game still portrays the violent and destructive actions committed by the characters as necessary for social change. DedSec may look, talk, and think like hacktivists, but DedSec's actions do not always align with the values and ethics of hacktivists. It is understandable of Ubisoft to believe that digitally recreating nonviolent protest would not entertain its audience, but DedSec earning social changes without resorting to violent and destructive acts would have sent a stronger message. Letting players commit acts of violence for financial gain in the name of hacktivism does a disrespect to actual hacktivists.

While this article is grounded in literature about hacker culture and hacktivism, the analytic part mostly ignores factors outside of *Watch Dogs 2* such as real-world markets and events that may have influenced the creation of the text. The article also ignores the audience reception of the game. Thus, a production analysis or a reception study on *Watch Dogs 2* would be valuable for further understanding the game's representation of hacker culture and hacktivism. Other possible research directions include examining other games about hacking and comparing their messages and gameplay mechanics to *Watch Dogs 2*. Another direction could be examining a text about hacking that is in a medium different from video games. One could investigate what themes and representations are common across media about hacking.

John J. Fennimore is an award-winning writer and scholar. He is a graduate of the Media Studies master's program at the University of Wisconsin-Milwaukee and is

an incoming student of the Communication, Rhetoric and Digital Media PhD program at North Carolina State University. He is intrigued by the commercial aspects of video games, the psychology of players, and the power dynamic between players and video game corporations. His master's thesis explores the impact of cosmetic items on the gameplay and game design of Fortnite. He's written over 1,000 articles and gained over 11 million pageviews for the gaming, entertainment, and news sections of real-time information platform Heavy.com. He's presented at the Midwest Interdisciplinary Graduate Conference 2020 & 2021, the DePaul University Pop Culture Conference 2019 & 2021, and Global Fusion 2019 where he won third place in the student paper competition. His favorite games are *Hades*, *Bloodborne*, *Bayonetta 2*, *Undertale*, *Nioh* 2 and *Yoshi's Island*.

REFERENCES

Ali Saifudeen, O. (2021). Hacking the hacker's psyche. In M. Khader, W. Xiau Ting Chai, & L. Seng Neo (Eds.), *Introduction to cyber forensic psychology: Understanding the mind of the cyber deviant perpetrators* (pp. 267-285). Singapore: World Scientific Publishing Company. https://doi.org/10.1142/9789811232411_0013

Bankhurst, A. (2020, July 12). Ubisoft will not directly address abuse allegations during ubisoft forward. *IGN*. https://www.ign.com/articles/ubisoft-will-not-directly-address-abuse-allegations-during-ubisoft-forward

Bogost, I. (2007). *Persuasive games: The expressive power of videogames*. Boston: MIT Press. https://mitpress.mit.edu/books/persuasive-games

Boluk, S. & Lemieux, P. (2017). *Metagaming: Playing, competing, spectating, cheating, trading, making, and breaking videogames*. Minneapolis: University of Minnesota Press. https://www.upress.umn.edu/book-division/books/metagaming

Clark, P. (2018, July 16). Update: Splatoon 2 leaderboard hacker banned by Nintendo indefinitely. https://www.ign.com/articles/2018/07/16/splatoon-2s-leaderboards-hacked-to-beg-nintendo-for-a-cheating-fix.

Coleman, G. E. (2013). *Coding freedom: The ethics and aesthetics of hacking*. Princeton, NJ: Princeton University Press. https://press.princeton.edu/books/paperback/9780691144610/coding-freedom

Collister, L. B. (2017). Transformative (h)activism: Breast cancer awareness and the World of Warcraft running of the gnomes. *Transformative Works and Cultures*, 25. http://dx.doi.org/10.3983/twc.2017.990

Denning, D. E. (2006). A view of cyberterrorism five years later. In K. Himma (Ed.), *Internet security: Hacking, counterhacking, and society*, 124. Burlington, MA: Jones and Bartlett Publishers.

Jaquet-Chiffelle, D.-O. & Loi, M. (2020). Ethical and unethical hacking. In M. Christen, B. Gordijn, & M. Loi (eds.), *The ethics of cybersecurity* (pp. 179-204). The International Library of Ethics, Law and Technology 21. Springer, Cham. https://doi.org/10.1007/978-3-030-29053-5_9

Kretzschmar, M. & Stanfill, M. (2019). Mods as lightning rods: A typology of video game mods, intellectual property, and social benefit/harm. *Social & legal studies 28*(4), 517-536. https://doi.org/10.1177/0964663918787221

Kubitschko, S. (2015). The role of hackers in countering surveillance and promoting democracy. *Media and Communication, 3*(2), 77-87. https://doi.org/10.17645/mac.v3i2.281

Levy, S. (2010). *Hackers: Heroes of the computer revolution*. Newton, MA: O'Reilly Media, Inc.

Malaby, T. M. (2007). Beyond play: A new approach to games. *Games and Culture, 2*(2), 95-113.

Manion, M., & Goodrum, A. (2000). Terrorism or civil disobedience: Toward a hacktivist ethic. *ACM SIGCAS Computers and Society, 30*(2), 14-19. https://doi.org/10.1145/572230.572232

Mansfield-Devine, S. (2011). Hacktivism: Assessing the damage. *Network Security, 2011*(8), 5-13. https://doi.org/10.1016/S1353-4858(11)70084-8

Murphy, D. (2013). Hacking public memory: Understanding the multiple arcade machine emulator. *Games and Culture, 8*(1), 43-53. https://doi.org/10.1177/1555412013478687

Newman, J. (2018). Kaizo Mario Maker: ROM hacking, abusive game design and Nintendo's Super Mario Maker. *Convergence, 24*(4), 339-356. https://doi.org/10.1177/1354856516677540

Nikitina, S. (2012). Hackers as tricksters of the digital age: Creativity in hacker culture. *The Journal of Popular Culture, 45*(1), 133-152. https://doi.org/10.1111/j.1540-5931.2011.00915.x

Pawlicka, A., Choraś, M. & Pawlicki, M. (2021). The stray sheep of cyberspace a.k.a. the actors who claim they break the law for the greater good. *Pers Ubiquit Comput*. https://doi.org/10.1007/s00779-021-01568-7

Postigo, H. (2008). Video game appropriation through modifications: Attitudes concerning intellectual property among modders and fans. *Convergence, 14*(1), 59-74. https://doi.org/10.1177/1354856507084419

Powell, A. (2016). Hacking in the public interest: Authority, legitimacy, means, and ends. *New Media & Society, 18*(4), 600-616. https://doi.org/10.1177/1461444816629470

Schreier, J. (2020, July 21). Ubisoft family accused of mishandling sexual misconduct claims. *Bloomberg Businessweek*. https://www.bloomberg.com/news/articles/2020-07-21/ubisoft-sexual-misconduct-scandal-harassment-sexism-and-abuse

Sitzes, J. & Petite, S. (2020, July 15). Last chance to get *Watch Dogs 2* for free on PC. *Gamespot*. https://www.gamespot.com/articles/last-chance-to-get-watch-dogs-2-for-free-on-pc/1100-6479419/

Söderberg, J. & Maxigas. (2021). The three pillars of functional autonomy of hackers. *Nanoethics, 15*, 43-56. https://doi.org/10.1007/s11569-021-00389-5

Tufekci, Z. (2017). *Twitter and tear gas: The power and fragility of networked protest*. New Haven, CT: Yale University Press. https://www.twitterandteargas.org/

Tuner, F. (2006). *From counterculture to cyberculture: Stewart Brand, the Whole Earth Network, and the rise of digital utopianism*. Chicago: University of Chicago Press.

Ubisoft. (2016). *Watch Dogs 2*. Ubisoft. https://www.ubisoft.com/en-us/game/watch-dogs/watch-dogs-2.

Watch Dogs 2 (PC version) [Video game]. (2016). Ubisoft.

Zhao, B. & Zhang, S. (2019). Rethinking spatial data quality: Pokemon Go as a case study of location spoofing. *The Professional Geographer, 71*(1), 96-108. https://doi.org/10.1080/00330124.2018.1479973