Computer Privacy

I. In the Hands of Responsible Authorities

Deep inside of Yucca Mountain gets stored a frightening proliferation of barrels of permanently disposed nuclear waste.[1] At least, this would be the case if the American public could reach the reasonable agreement[2] on a choice of location to store our nation's ever-increasing surplus of nuclear waste.[3] The waste is currently left to contaminate underdeveloped on-location temporary storage next to refineries. In the event of Yucca Mountain's theoretical usage, one might expect access to such a strategically invaluable location to be carefully protected. This protection must extend over to complex computer systems, where things can begin to go awry. A former employee of the Nuclear Regulatory Commission, described as having been "terminated" from his job, executed a simple email attack[4] against thousands of collected employee emails during Jan. 2015. This employee was alleged in court to have demanded private information in the email that could lead to the theft and sale of state nuclear secrets by posing as a trusted individual on the network, an attack commonly referred to as spear-phishing.

[1] *Yucca Mountain.org Eureka County, Nevada – Nuclear Waste Office*. Yucca Mountain Repository Project, 23 Mar. 2018, www.yuccamountain.org/index.htm.

[2] Collins, Michael. "Congress works to revive long-delayed plan to store nuclear waste in Yucca Mountain." *USA Today*, 3 Jun. 2018, www.usatoday.com/story/news/politics/2018/06/03/yucca-mountain-congress-works-revive-dormant-nuclear-waste-dump/664153002/.

[3] Berezow, Alex. "Yucca Mountain is the safest spot for nuclear waste. We should pay Nevada to use it." *USA Today*, 14 Jun. 2019, www.usatoday.com/story/opinion/2019/06/14/yucca-mountain-facility-should-used-store-nuclear-waste-column/1351433001/.

[4] Hsu, Spencer S. "Former Energy Dept. Employee Pleads Guilty in Nuclear Secrets Sting Case." *The Washington Post*, 3 Feb. 2016, www.washingtonpost.com/world/national-security/former-energy-dept-employee-pleads-guilty-in-nuclear-secrets-sting-case/2016/02/02/3b5a6f92-c930-11e5-ae11-57b6aeab993f_story.html.

Popular tech websites list spear-phishing as a low-level attack[5] and present simple defensive countermeasures that ordinary individuals can implement on their own, but it continues to be a source of numerous data breaches. The defendant, after being fired, is said to have went to officials of a foreign government offering to sell information to them, but they instead reported him to the FBI. He claimed in his defense that he was pressured by the FBI into carrying out a much more elaborate plan than the one he had personally conceived, which has come to be a common refrain in cases of cybercrime. U.S. intelligence agencies are actively engaged in many instances of cyber warfare that include social engineering of targets, as with the arrest of Jeremy Hammond whose conviction[6] for computer hacking during the track down of the group Anonymous resulted from heavy communication with FBI operatives, and other methods[7] which now often directly involve US citizens.[8] A few years prior, U.S. and Israeli intelligence agencies successfully deployed an attack[9] that included the use of a series of zero-day (or previously unknown) vulnerabilities to move their virus payload onto computer controllers for the centrifuges of an Iranian nuclear facility.

In another incident, 30 instructors were suspended from the U.S. Navy nuclear propulsion school in Feb. 2014, after having been caught cheating on exams.[10] This was preceded by 90 officers from the U.S. Air Force's nuclear weapons corps involved in a prior unconnected cheating scandal.[11] At the very top level, we are not able to maintain the reasonable expectation that individuals observe proper safety protocols governing the most fragile of institutions.

[5] Palmer, Danny. "What is phishing? Everything you need to know to protect yourself from scam emails and more." *ZDNet*, 6 Sept. 2017, www.zdnet.com/article/what-is-phishing-how-to-protect-yourself-from-scam-emails-and-more.

[6] Hedges, Chris. *Wages of Rebellion: The Moral Imperative of Revolt.* Nation Books, 2016, p. 216.

[7] Ackerman, Spencer and James Ball. "NSA loophole allows warrantless search for US citizens' emails and phone calls." *The Guardian*, 9 Aug. 2013, www.theguardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls.

[8] Poitras, Laura and James Risen. "N.S.A. Gathers Data on Social Connections of U.S. Citizens." *The New York Times*, 28 Sept. 2013, www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html.

[9] Nakashima, Ellen and Joby Warrick. "Stuxnet was work of U.S. and Israeli experts, officials say." *The Washington Post*, 2 June 2012, www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.

[10] Stewart, Phil. "U.S. Navy investigating sailors over nuclear exam cheating." *Reuters*, 5 Feb. 2014, www.reuters.com/article/us-usa-nuclear-cheating-idUSBREA1400J20140205.

[11] Memmott, Mark. "Air Force Cheating Scandal Widens; 92 Nuclear Officers Linked." *NPR*, 30 Jan. 2014, www.npr.org/sections/thetwo-way/2014/01/30/268880352/air-force-cheating-scandal-widens-to-92-nuclear-officers.

One former officer has said[12] the following:

> This falsified value, reminiscent of the hollow financial markets before the crisis, was covered up by the admirals' apparent maxim: When in doubt, obfuscate! Everything was stamped top secret, so only the insiders could read what was happening. Not even Congress knows the true extent of the submarine force and its inconspicuous irrelevance …
>
> … In fact, every classified document I ever read in the submarine force could replace the word SECRET with another six-letter word—BORING.

The development of encryption has in many ways paralleled that of nuclear power, which after starting out as a weapon has severely hampered its application in other domains and led the public to view it with distrust. No matter whether reactor design can be made safe as some sources indicate[13], its coupling with computer networks and their operators has led to some trouble. It might be that the security of not only mountains of nuclear waste, but also remaining stockpiles of nuclear weapons provide good reason for the creation of much stronger encryption algorithms to protect the computer controllers of these and other industrial systems. US nuclear policy has been redrafted in 2018 to expand use of nuclear weapons in counterattacks against non-nuclear forces, and to build the first new nuclear weapons since the end of the Cold War.[14] Incredibly, the US and Russia are re-escalating an arms race[15] all while cooperating[16] extensively[17] within the field of world geopolitics, juggling 50 nuclear bombs that remain in Turkey even while their original purpose as a Soviet deterrent now appears to be entirely obscured. Whether future democratic efforts may overcome this historically bipartisan effort to induce nuclear terror into the American public has not been decided.

[12] Brownfield, Christopher. "The Submarine Nuclear Scandal." *Newsweek/The Daily Beast*, 22 Sept. 2010, www.thedailybeast.com/articles/2010/09/22/the-submarine-nuclear-scandal.html.

[13] Martin, Richard. "Fail-Safe Nuclear Power." *MIT Technology Review,* 2 Aug. 2016, www.technologyreview.com/s/602051/fail-safe-nuclear-power.

[14] Sanger, David E. and Broad, William J. "Pentagon suggests being ready to counter devastating cyberattacks with nuclear arms." Boston Globe, 16 Jan. 2018, www.bostonglobe.com/news/nation/2018/01/16/pentagon-suggests-being-ready-counter-devastating-cyberattacks-with-nuclear-arms/U70hYcUeaYgR6IgPYcfW5H/story.html.

[15] Pazzanese, Christina. "Stirrings of a new nuclear arms race." *The Harvard Gazette*, 1 Mar. 2018, news.harvard.edu/gazette/story/2018/03/stirrings-of-a-renewed-nuclear-arms-race/.

[16] Broad, William J. and Sanger, David E. "Erdogan's Ambitions Go Beyond Syria. He Says He Wants Nuclear Weapons." *The New York Times*, 20 Oct. 2019, www.nytimes.com/2019/10/20/world/middleeast/erdogan-turkey-nuclear-weapons-trump.html.

[17] Cohen, Zachary. "Trump appears to confirm open secret about US nuclear weapons in Turkey." *CNN*, 16 Oct. 2019, www.cnn.com/2019/10/16/politics/trump-us-nuclear-weapons-turkey/index.html.

Accordingly, the US is alleged to have spent at least $50 billion dollars during 2013 on its black budget funding of what journalists for the Washington Post called an, “Intelligence-gathering colossus.”[18] We will see that they have managed to undermine their own security quite extensively. Even more critically, attempts by the US made at thwarting the export of encryption systems they do not retain backdoor access to have been repeatedly resisted by hackers acting largely in an individual capacity and while holding considerably fewer resources at their disposal.[19] The state’s treacherous sabotage of encryption schemes, widely used both by corporations internationally and US citizens themselves, has become divulged by no more than a midranking contractor-turned whistleblower.[20]

After discussing issues of commercial encryption products, we will examine a paradox concerning the human rights activists’ need for open access to encryption algorithms. At the same time, we should expect corporations working in the defense industry to produce a countervailing line of decryption tools designed to interfere with perceived forms of seditious communication. It can be observed that both an active ongoing arms race and an accompanying escalation in conflict regarding encrypted computer systems and their disruption are taking place. This is being done on the part of the state police, corporations, and other unaffiliated hackers; demilitarization of these systems will not likely happen without offering real alternatives for the reinvestment of volatile forces already existing in the world.

II. Corporate Encryption Escalation

US-based retail store Target lost the personal information of at least 70 million customers in Nov. 2013, due to a simple breach of its credit card systems.[21] Its security team was alerted about

[18] Gellman, Barton and Greg Miller. “ ‘Black Budget’ Summary Details U.S. Spy Network’s Successes, Failures and Objectives.” *The Washington Post*, 29 Aug. 2013, www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html.

[19] Back, Adam. “export-a-crypto-system.” *Cypherspace*, 1 Sept. 2003, www.cypherspace.org/rsa.

[20] Greenwald, Glenn, Evan MacAskill, and Lauren Poitras. “Edward Snowden: the whistleblower behind the NSA surveillance revelations.” *The Guardian*, 11 June 2013, www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

[21] Geuss, Megan. “Judge Rules That Banks Can Sue Target for 2013 Credit Card Hack.” *Ars Technica*, 5 Dec. 2014, arstechnica.com/tech-policy/2014/12/judge-rules-that-banks-can-sue-target-for-2013-credit-card-hack.

an impending attack prior to its event and did nothing in response. Target has reached a settlement in the case and agreed to pay a $10 million fine[22], valuing the data of its customers at $0.14 each. Another recent attack[23] on Home Depot shows the extent to which security measures taken to guard customer data fails to meet the meager standards large companies even bother to set for themselves. Although they claim[24] that, “Protecting our customers’ information is something we take extremely seriously,” it has been argued in one of at least forty lawsuits filed in both the US and Canada that the personal data and credit card information of 50 million customers could only end up discovered for sale on the black market because of their servers missing all security measures entirely. These kinds of incidents are becoming increasingly regular - with the greatest breaches[25] numbering in the hundreds of millions to billions of accounts harvested in total.

Worse cases of malfeasance involve computer hardware shipped with vulnerabilities designed directly embedded into the circuitry before programs running on them are able to be attacked. It has been speculated the Meltdown/Spectre vulnerabilities, found in 2017 existing for decades[26] in both Intel and AMD processors, have the look of something U.S. intelligence agencies ordered be deliberately introduced into the hardware level of nearly all modern computer processors. A White House spokesman responded[27] of course, that, “…the U.S. government would never put a major company like Intel in a position of risk.” It is not unheard of though for the US or its equivalent agencies internationally to introduce vulnerabilities that are difficult or even impossible to identify through analysis of running code.

[22] “Target Agrees to Pay $10 Million to Data Breach Victims.” *CBS News*, 18 Mar. 2015, www.cbsnews.com/news/target-reaches-proposed-settlement-with-data-breach-victims.

[23] Farivar, Cyrus. “Home Depot Hit with ‘at Least 44 Civil Lawsuits’ Due to Data Breach.” *Ars Technica*, 25 Nov. 2014, arstechnica.com/tech-policy/2014/11/home-depot-hit-with-at-least-44-civil-lawsuits-due-to-data-breach.

[24] Lemos, Robert. “Home Depot investigates potential hacking of credit card data.” *Ars Technica*, 3 Sept. 2014, arstechnica.com/information-technology/2014/09/problems-at-home-home-depot-investigates-potential-breach.

[25] Weise, Elizabeth. “USA TODAY’s list of the biggest data breaches and hacks of all time.” *USA Today*, 3 Oct. 2017, www.usatoday.com/story/tech/2017/10/03/biggest-data-breaches-and-hacks-all-time/729294001.

[26] Moore-Colyer, Roland. “Intel, ARM and AMD all affected by security-bypassing, kernel-bothering CPU bugs.” *The Inquirer*, 4 Jan. 2018, www.theinquirer.net/inquirer/analysis/3023798/intel-arm-and-amd-all-affected-by-meltdown-and-spectre-security-bypassing-cpu-design-flaw.

[27] Dwoskin, Elizabeth, Hamza Shaban, and Craig Timberg. “Huge security flaws revealed — and tech companies can barely keep up.” *The Washington Post*, 5 Jan. 2018, www.washingtonpost.com/business/technology/huge-security-flaws-revealed–and-tech-companies-can-barely-keep-up/2018/01/05/82ccbe18-f24e-11e7-b3bf-ab90a706e175_story.html.

Due to most hardware devices having much stricter IP protections than their accompanying codebases[28], researchers have struggled[29] with developing methods to search for vulnerabilities in them, deliberately planted or otherwise. After the 2014 discovery of the Heartbleed vulnerability contained in the encrypted networking library OpenSSL, security company Symantec warned[30] that, "…hardware devices are not immune to the vulnerability. It can affect routers, PBXes (business phone systems) and likely numerous devices in the Internet of Things." Although their commitment to providing customers a quick solution to the vulnerability was admirable, they leave out the detail of how the NSA exploited the vulnerability for two years[31] before disclosing it to vendors for a fix - wildly endangering many people.

The NSA directly influenced the design of standard library encryption algorithms[32] under the guise of its work with other organizations following the procedures set in place by mandatory export control laws. This has allowed them to potentially introduce their own extra sets of backdoor private keys into those algorithms, offering immediate access to much of the encrypted traffic being sent across the internet already gathered in bulk[33] through cooperation with ISPs like AT&T. Differing security researchers have contested whether the NIST, a US government agency responsible for oversight of the standard library used widely around the world, should have been aware of the mathematical vulnerability inherent in their algorithm at the time of its creation. Another option is that the NSA by its own research later on came across the previously unknown vulnerability.

They would then exploit weaknesses in the mathematical constants selected as parameters for the algorithm using $100 million-dollar supercomputers to crack the private keys of captured net-

[28] Terdiman, Daniel. "Open-source hardware standards formally issued." *CNET*, 13 July 2010, www.cnet.com/news/open-source-hardware-standards-formally-issued.

[29] Zammit, Damien. "Intel x86s hide another CPU that can take over your machine (you can't audit it)." *Boing Boing*, 15 June 2016, boingboing.net/2016/06/15/intel-x86-processors-ship-with.html.

[30] Chien, Eric. "Heartbleed Poses Risk to Clients and the Internet of Things." *Symantec*,14 Apr. 2014, www.symantec.com/connect/blogs/heartbleed-poses-risk-clients-and-internet-things.

[31] Zetter, Kim. "Report: NSA Exploited Heartbleed to Siphon Passwords for Two Years." *Wired*, 11 Apr. 2014, www.wired.com/2014/04/nsa-exploited-heartbleed-two-years.

[32] Zetter, Kim. "How a Crypto 'Backdoor' Pitted the Tech World Against the NSA." *Wired*, 24 Sept. 2013, www.wired.com/2013/09/nsa-backdoor.

[33] Angwin, Julia, Jeff Larson, Henrik Moltke, Laura Poitras, James Risen, and Charlie Savage. "AT&T Helped U.S. Spy on Internet on a Vast Scale." *The New York Times*, 15 Aug. 2015, www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html.

work traffic, for all key lengths up to the level of present-day recommended practices. Regardless, it seems almost certain the NSA has somehow become aware of the vulnerability[34], and more research must be aimed at the mathematical nature of vulnerabilities contained in encryption algorithms beyond just the much more apparent faults in their implementation. It would be almost impossible to prove that a private key does exist in the wild for this class of widely used encryption algorithm, except that its corresponding network traffic was being decrypted in bulk, whereas given possession of a private key that was either generated along with the algorithm or brute forced later on, all network traffic employing that algorithm could be quickly decrypted in a way that would go undetected.

There are arguments concerning exactly how many zero-day vulnerabilities the US retains secret access to, but they number at least somewhere in the tens to hundreds at any given time and it is calculated for them to have underreported[35] this figure in the past. We can also see in the recent Apple - FBI case that it would seem government intelligence agencies do not yet completely possess the total oversight[36] they would prefer to have. The latest updated operating system running on iPhones has encryption built-in by default which has been rare among device manufacturers when not faced with legal pressure. FBI lawyers were blocked in court from ordering Apple to unlock the encrypted phone, before they outsourced the job to an unknown contractor group in possession of their own proprietary hacking tool. The tool reportedly cost the FBI over a million dollars for one time use and was not ultimately disclosed to them, finally allowing them to break the encryption of the phone without legal authorization.[37] Courts have nonetheless shown some resolve regarding the protection of personal data even in sometimes extreme instances out of a shared commitment to its observation as a human right.

[34] Hales, Thomas C. “The NSA Back Door to NIST.” *Notices of the American Mathematical Society*, vol. 61, no. 2, Feb. 2014, DOI: 10.1090/noti1078, pp. 190-192.

[35] Zetter, Kim. “US Used Zero-Day Exploits Before It Had Policies for Them.” *Wired*, 30 Mar. 2015, www.wired.com/2015/03/us-used-zero-day-exploits-policies.

[36] Nakashima, Ellen. “Apple vows to resist FBI demand to crack iPhone linked to San Bernardino attacks.” *The Washington Post*, 17 Feb. 2016, www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99_story.html.

[37] Zapotosky, Matt. “FBI has accessed San Bernardino shooter’s phone without Apple’s help.” *The Washington Post*, 28 Mar. 2016, www.washingtonpost.com/world/national-security/fbi-has-accessed-san-bernardino-shooters-phone-without-apples-help/2016/03/28/e593a0e2-f52b-11e5-9804-537defcc3cf6_story.html.

Law student Max Schrems won another case tried in Irish courts[38], where Facebook's Europe HQ is located, preventing the company from storing data of its European users in the US as a result of privacy concerns stemming from mass surveillance spying. This affords better protections for citizens of EU member countries, though it remains unclear how all relevant privacy concerns could become resolved fairly along national boundary lines. Many internet companies operate servers located in multiple countries, conduct international business across their boundaries, and as a consequence are required to work with the identifying credentials of customers in order to secure transactions. While data ostensibly may not be stored on servers in countries where privacy rights are ignored, enough data continues to be sent across those compromised networks that it provides minimal protections for personal data that would have been abused either way. In view of the international nature of the internet, only regulations existing with such a broad scope could provide legitimate protection for the privacy rights of all internet users. The EU has gone further to plan general regulations[39] guarding the export of personal data, and to affirm the right to erase historically obtained personal data from its companies' servers. It is currently being decided[40] whether these rights extend to citizens or non-citizens residing presently in non-EU member countries.

In his guide to personal privacy protection[41], renowned hacker Kevin Mitnick argues that, "The danger of living within a digital surveillance state isn't so much that the data is being collected (there's little we can do about that) but what is done with the data once it is collected." He then goes on to present plausible cases in which complex analysis of data performed on the profiles of large numbers of people will lead to outcomes affecting yourself as an individual when your amassed personal data could otherwise be viewed as mundane. These factors are magnified for data harvesters by generating relational maps from the networks of people we choose to interact

[38] Fioretti, Julia, Francois Murphy, and Shadia Nasralla. "Max Schrems: the law student who took on Facebook." *Reuters*, 7 Oct. 2015, www.reuters.com/article/us-eu-ireland-privacy-schrems/max-schrems-the-law-student-who-took-on-facebook-idUSKCN0S124020151007.

[39] *Data protection Rules for the protection of personal data inside and outside the EU.* European Commission, ec.europa.eu/info/law/law-topic/data-protection_en.

[40] Hern, Alex. "ECJ to rule on whether 'right to be forgotten' can stretch beyond EU." *The Guardian*, 20 July 2017, www.theguardian.com/technology/2017/jul/20/ecj-ruling-google-right-to-be-forgotten-beyond-eu-france-data-removed.

[41] Mitnick, Kevin David and Robert Vamosi. *The Art of Invisibility: the World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data.* Little, Brown and Company, 2017, p. 16.

with, further illuminating our own habits and preferences as part of a manageable broader culture. That is to say it's not a question of whether your information is free, but how it's being used.

Before the Cambridge Analytica story broke a year later, the journalist Jonathan Albright was already reporting in Nov. 2016 on how an insular social media activity propagation machine[42] was being devised in order to convince a crowd of their membership to a burgeoning club and mutual belonging in it through engagement with low budget, politically charged brand accounts. This was being done deliberately to pinpoint the target group's proclivity to engage with social media pages, not to help congregate together a grassroots democratic movement but to conduct metrics on the audience's personal data. These profiles then get matched to individuals with hyper-specific microtargeted political ads, uniquely crafted to prey on the emotions of undecided voters leading up to the end of a run-off election most likely to swing a decision. Sociologist professor Zeynep Tufekci argues this will lead to politics becoming more attentive to differences on the margins[43] often decided as inflamed wedge issues. As recently as Apr. 2018, calls were being made in the press[44] for an increased public interest to be shown concerning the privacy rights of users on widely used websites like Facebook. It is now revealed that the profiles of billions of users have been obtained by malicious parties[45] through what were made to be easily accessible API search functions intended for potential advertisers.

Kaan Kangal has argued, in response to work on Christian Fuchs' Marxist engagement with digital media, that users in fact produce no value.[46] All of the value is held in the systems that analyze and process the data as raw input, which on its own can not be sold as commodity for any of the intended analytical purposes. It is the labor power of the workers who design the systems

[42] Albright, Jonathan. "#Election2016: Propaganda-lytics & Weaponized Shadow Tracking." *Medium*, 22 Nov. 2016, medium.com/@d1gi/election2016-propaganda-lytics-weaponized-shadow-trackers-a6c9281f5ef9.

[43] Tufekci, Zeynep. "Engineering the public: Big data, surveillance and computational politics." *First Monday*, vol. 19, no. 7, 7 July 2014, www.firstmonday.dk/ojs/index.php/fm/article/view/4901/4097.

[44] Rich, Jessica. "Beyond Facebook: It's High Time for Stronger Privacy Laws." *Wired*, 8 Apr. 2018, www.wired.com/story/beyond-facebook-its-high-time-for-stronger-privacy-laws.

[45] Dwoskin, Elizabeth, Tony Romm, and Craig Timberg. "Facebook: 'Malicious actors' used its tools to discover identities and collect data on a massive global scale." *The Washington Post*, 4 Apr. 2018, www.washingtonpost.com/news/the-switch/wp/2018/04/04/facebook-said-the-personal-data-of-most-its-2-billion-users-has-been-collected-and-shared-with-outsiders.

[46] Kangal, Kaan. "The Karl Marx Problem in Contemporary New Media Economy: A Critique of Christian Fuchs' Account." *Television & New Media*, vol. 17, no. 5, Jan. 2016. pp. 7-8.

to process the data that gets commodified and sold to capitalists in exchange for a wage, with the included surplus being appropriated by the capitalist. This leads to an circular struggle between a slight misreading of Marx about the source of surplus value production, and an apparent Autonomist rejoinder that the goal would be to move beyond relying on surplus value to drive production and in fact in the modern age of democraticized labor power we have now already achieved this - to be followed by further developments. Fuchs in turn has responded to the Autonomist critique of Marx's "Fragment on Machines" in the *Grundrisse*, a key text on the subject where he claims Marx theorizes an early form of a "global information network",[47] which he then applies to Eatwell, Hardt, Negri, Robinson, Sraffa, Vercellone, and Virno, among others, while siding with the reading of Postone and Rosdolsky[48], that:

> …when he speaks of a breakdown in the Fragment, Marx does not mean an automatic collapse of capitalism, but rather that exchange value collapses within communism and that the rise of knowledge work and automation bring about a fundamental antagonism of necessary labour time and surplus labour time. The establishment of communism however presupposes a conscious revolutionary sublation of capitalism.

So we can see that under these conditions of automation and rising knowledge work, as described, there is a general breakdown in exchange value, but this can not itself lead to communism without a "conscious revolutionary sublation of capitalism". The AI NOW Institute's 2017 report[49] concludes that even with the combination of AI, big data, and algorithms having an increasing beneficial impact on society, care must still be shown in respect to their effects on human rights, specifically for those living in poverty. Their recommendations include that commercial or in-house black box AI and algorithmic systems stop being used. This is due to how they are made to be averse to public auditing of their internal design and so cannot be held to normal accountability standards. Furthermore, they are well-documented as being used to target minority populations for intensive surveillance in violation of civil liberties. Since we are prone to viewing privacy only in terms of its bounds on other human prying eyes, we fail to see the extent to which

[47] Fuchs, Christian. "Marx's Capital in the Information Age." *Capital & Class*, vol. 41, no. 1, 2016. pp. 6-11.

[48] Fuchs, Christian. "The Information Economy and the Labor Theory of Value." *International Journal of Political Economy*, vol. 46, no.1, 2017. pp. 69-70.

[49] Campolo, Alex, Kate Crawford, Madelyn Sanfilippo, and Kate Crawford. "AI Now 2017 Report." *AI Now Institute*, Oct. 2017, pp. 28-32.

computer algorithms operating on enormous datasets are able to make effective predictions about habitual behavior as it pertains in aggregate to uniquely identifiable cross-sections of individuals drawn from mass populations.

This new model exceeds limitations intrinsic to the old individual rights based discourse intended to resolve classical privacy issues. In multiple recent articles, researchers have argued that while industry standard practice demands a "persistent identity ecosystem" for a number of reasons beneficial for the needs of business, there are documented positive[50] psychological[51] effects[52] obtaining for networks of users where privacy is guaranteed as a fundamental right. Researchers have argued that in light of the inability to opt-out from general data collection during daily affairs, individual members of the public should move to obfuscating the trace of their own data trail by encrypting or otherwise mangling the metadata that web browser and other mobile applications are able to collect.[53] While this method can never be perfect, it at least offers a better solution than hoping our actual personal data will ever be managed correctly were it only to start being priced the right way.

III. The Right to Be Left Alone

In the 1890 *Harvard Law Review* article "The Right to Privacy", we discover a source of the historical roots of privacy as it was originally understood in regard to American law.[54] These authors formulate at least in part what remains of the privacy ideals still held on to. Although they examined how existing intellectual property law might provide for a foundational notion, they conclude that it pertains only to the decision of publication and is therefore a special case of the much more

[50] Donath, Judith S. "Identity and Deception in the Virtual Community." *Communities in Cyberspace*, Routledge, pp. 29-59.

[51] Bodle, Robert. "The ethics of online anonymity or Zuckerberg vs. 'Moot'." *Computers and Society*, vol. 43, no. 1, ACM, May 2013, pp. 22-30.

[52] Iane, Corina. "Anonymity On The Internet And Its Psychological Implications For Communication." *Cercetări filosofico-psihologice*, vol. 3, no. 2, 2011, pp. 125-131.

[53] Brunton, Finn and Nissenbaum, Helen. "The Fantasy of Opting Out." *THE MIT Press Reader*, 25 Sept. 2019, thereader.mitpress.mit.edu/the-fantasy-of-opting-out/.

[54] Brandeis, Louis and Samuel Warren. "The Right to Privacy." *Harvard Law Review*, vol. 4, no. 5, 15 Dec. 1890, pp. 193-220.

general right to be left alone, or the freedom to choose when to withhold thought. Thomson argued later in 1975 that still after all of the development until then, "Nobody seems to have any clear idea of what the right to privacy is."[55] Lacking an immediate definition though does not strictly deny there being any justice following from the concept. She proceeds through a number of scenarios that are supposed to lead us to the skeptical understanding that, "It is possible to explain in the case of each right in the cluster how we come to have it without ever mentioning the right of privacy."[56] In this way the right to privacy may not be a simple idea to express but it can always in each case be grounded in other concepts it is implicitly connected to.

Many people resist any type of demand for this expansion in the terms of responsibility concerning one's own privacy. Up until now, it has been made an overly complicated matter and often can be unclear for the public as to how it must be incorporated into a life more broadly. The dark net, for example, is a network existing on top of the internet that can only be accessed using special applications like the Tor Browser software. In a recently conducted poll, 70% of American respondents replied that they would want the dark net shut down, presumably having been convinced that it is a vehicle for drug dealers, terrorists, and child predators to congregate together without facing apprehension by the police. Following from this public sentiment, US senators Burr and Feinstein attempted to introduce the "Compliance with Court Orders Act of 2016", requiring companies like Apple and Google to introduce backdoor decryption methods into their devices so that law enforcement can forcibly enter them when necessary. Feinstein said that, "Silicon Valley has to take a look at their products, because if you create a product that allows evil monsters to communicate in this way—to behead children, to strike innocents, whether it's at a game in a stadium, in a small restaurant in Paris, take down an airliner—that's a big problem." If a backdoor can be used by the government or by anyone it deems as responsible, it also necessarily reduces the complexity to attack[57] compared with the primary source of encryption by the very criminals said to be the cause

[55] Thomson, Judith Jarvis. "The Right to Privacy." *Philosophy and Public Affairs*, vol. 4, no. 4, 1975, p. 312.

[56] Thomson, p. 313.

[57] Abelson, Harold; Anderson, Ross; Bellovin, Steven M.; Benaloh, Josh; Blaze, Matt; Diffie, Whitfield; Gilmore, John; Green, Matthew; Landau, Susan; Neumann, Peter G.; Rivest, Ronald L.; Schiller, Jeffrey I.; Schneier, Bruce; Specter, Michael; Weitzner, Daniel J. "Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications." *Dspace@MIT*, 6 July 2015, pp. 1-25.

of overwrought anxieties.

US intelligence agencies, responsible for safeguarding Americans against such a dangerous consortium of hostile foreign powers, selectively target hackers who they allege as criminals are opposed to national security interests, the philosopher Peter Ludlow argues in “The Strange Case of Barrett Brown”.[58] At the same time, and often instigating participation in exactly these same cases, they directly finance and sanction the actions of other hacker groups purported to be working on the side of national security. Brown, like Hammond, was arrested for involvement in the hack of the NSA contractor company Stratfor that, among other nefarious activities reported in leaked emails, conducted surveillance of American citizens not charged with any crimes. As the hack was seen through to its completion and led by an FBI informant, many NSA operatives and personnel of related contractor agencies had compromising personal data included in the ensuing leak. The government has proven then it takes no issue with provoking obvious and unnecessary national security risks that couldn’t even have arisen in the first place, out of an increasingly misguided effort to keep the internet under control.

Significant privacy rights and the protection of them, so much as they are carefully outlined by security experts working in the media, won’t actually be provided in the fullest sense that is required for both the public and for smaller radical groups, because of how they reliably get ignored. Eric Hughes, author of the 1993 “Cypherpunk’s Manifesto”, argues[59] that, “For privacy to be widespread it must be part of a social contract.” Steeped in a 20th century American ideological blend of libertarian and anarchist ideals, like much of the rest of the subversive internet, it focuses on how new markets opened up by technology will lead to the free and open exchange of information – unless government overreach is allowed to block its ascent. They are right to say that the design of new privacy-focused technologies might include certain radical notions of rights that must be permitted, but this will not itself consist in the labor of writing, publishing, and double-checking the computer code on which these experiments will get built.

[58] Ludlow, Peter. “The Strange Case of Barrett Brown.” *The Nation*, 18 June 2013, www.thenation.com/article/strange-case-barrett-brown.

[59] Hughes, Eric. “Cypherpunk’s Manifesto.” *Activism.net*, 9 Mar. 1993, www.activism.net/cypherpunk/manifesto.html.

In a 1995 issue of *Social Philosophy & Policy*, David Friedman identified that communications would be performed on widely available modern desktop computers (PGP had been invented in 1991), and that people would meet from across the world in virtual reality rooms using these encrypted communication algorithms where as he said, "Changes currently in progress should result, over a decade or two, in a network with sufficient bandwidth to support real time audio-video for most users."[60] Give that, as he goes on, "…to my sight and hearing, it might as well be real," this would allow for it to address such communicative activities as "consulting, teaching, [and] meeting." But does this cover "a large fraction of human interactions," or more broadly, some large portion of the production process? It is notable that he then goes on to describe his idea of an early form of encrypted "digital" cash, whereas the Bitcoin network was started in 2009 and only later became more widely known after several years. He does notice that the Clipper Chip represents a sort of necessary kind of government response to public attempts at encryption, but that it will inevitably fail. This will happen when it is shown to subvert its own apparent purposes by exposing every person to the encroachment of spying, while leaving criminals to breezily protect their communications with an additional layer of manual encryption.

Though computer algorithms presently bring about outcomes of ambiguous nature, primarily when it comes to serving particular interests against others, the discovery and implementation of stronger, as yet unknown algorithms may bring competing parties together. Algorithms can be thought of as being used for producing spaces on the internet where novelty develops, rather than for the protection, sorting, and storage of information. Therefore, when Elon Musk haughtily proclaims that his Neuralink brain-computer interface could "solve" autism and schizophrenia, he should be reminded that these subjects cannot be made unconstrained of illness by having their actions or habits reinterpreted through a device in which all of the new degrees of freedom eerily subsist.[61] Friends of Musk, such as climate change skeptic Dr. Jay Lehr, have declared him "Brilliant at

[60] Friedman, David. "A World of Strong Privacy: Promises and Perils of Encryption." *Social Philosophy and Policy*, vol. 13, no. 2, 1996, pp. 212-228.

[61] Hamilton, Isobel Asher. "Elon Musk said his AI-brain-chips company could 'solve' autism and schizophrenia." *Business Insider*, 14 Nov. 2019, www.businessinsider.com/elon-musk-said-neuralink-could-solve-autism-and-schizophrenia-2019-11.

gaming the system."[62] And while there were already a slew of other reprehensible incidents he might have been held in contempt for, this was of course one week before it came out that he had paid $50,000 to a notorious fraudster for help with recovering information that doesn't exist.[63]

IV. Video Game Server Restoration

Online games are faced with the problem of maintaining a very short shelf-life before becoming officially shut down, which then must get salvaged by former communities of players[64] if they are to endure. There is a long history of game companies taking legal action against fan projects in order to maintain overall protection of their IP. It is being challenged in court on the basis of an alleged consumer right to preserve abandoned games[65], following from right to repair laws, in addition to the obvious academic implications that come along with impeding an unexplored avenue for anthropological research. Industry lobbyists warn that activists fighting for the preservation of these games, "…appear interested in allowing the public to play video games." Fan project games utilizing encryption could furthermore receive international play in defiance of often draconian and absurdly contradictory regional publishing restrictions, which sometimes prevent people who purchased legitimate copies of the game from playing together. In either case, the significance for our purposes resides in how it would stimulate a place of temporary activity to emerge and not the sanctioning off of valuable protected identities.

We might consider rebuilding for games a distributed client, referred to here as peer-to-peer or p2p, that does not rely on a constant connection to a central server but instead spreads computational responsibility out to all of the clients. When there is no central server to rely on, all clients

[62] Lehr, Jay and Prelutsky, Burt. "Elon Musk: Brilliant at gaming the system." *Committee For A Constructive Tomorrow*, 8 Sept. 2019, www.cfact.org/2019/09/08/elon-musk-brilliant-at-gaming-the-system/.

[63] Mac, Ryan. "Elon Musk Hired A Convicted Felon To Investigate The Cave Rescuer Who Is Now Suing Him." *BuzzFeed News*, 3 Oct. 2019, www.buzzfeednews.com/article/ryanmac/elon-musk-hired-felon-james-howard-higgins-dirt-pedo-guy.

[64] "International Center for the History of Electronic Games." *National Museum of Play*, www.museumofplay.org/about/icheg.

[65] Orland, Kyle. "Game industry pushes back against efforts to restore gameplay servers." *Ars Technica*, 21 Feb. 2018, arstechnica.com/gaming/2018/02/preservation-or-theft-historians-publishers-argue-over-dead-game-servers.

must agree on what kind of data will get shared and how its accurate transmission will be validated. This solution potentially introduces unreasonable latency and requires more to be done to achieve a sufficient implementation but could serve as the basis for similar p2p client applications made both for games and also other domains[66] where encrypted, high speed networking would be seen as useful. Traffic being sent between clients should be encrypted and anonymized as much as possible, which is achievable with readily available encryption schemes but might end up introducing further latency issues or complexity in design that presents negative effects for networks like those controlling high speed real time games. In an early example of such a system founded on games, in 2001 developers of *Age of Empires* released an article in the popular magazine Gamasutra detailing a method for controlling the realistic movement of 1500 archers in formation during a networked game of up to 8 players.[67] This sort of network traffic has not been well-studied yet still as ordinarily, encrypted traffic is considered slow-moving and is made specifically to meet other more pressing constraints, which generally rule out the real time transmission of common datatypes. Existing applications like Signal[68], for private messaging with primitive support for video calls, or BitTorrent[69], which transfers bulk data at high speeds but without the guarantee of immediate sequential delivery preventing content streaming in real time, have aimed to solve different specialized versions of this problem.

It is unfortunately easy then to get drawn in to a service showing fast growth that inevitably subverts its own ends through the demands of private equity. So, we find that while Facebook's Whatsapp API (purportedly now used by 1.5 billion users worldwide) was based purely on open source XMPP and Signal code, they repeatedly sent DMCA claims to any projects working with the code until it became unusable, leaving only their own proprietary and highly questionable client

[66] Wierzbicki, Adam. *Trust and Fairness in Open, Distributed Systems*. Springer Berlin Heidelberg, 13 Nov. 2014, pp. 1-7.

[67] Buttner, Paul and Terrano, Mark. "1500 Archers on a 28.8: Network Programming in Age of Empires and Beyond." *Gamasutra*, 22 Mar. 2001, www.gamasutra.com/view/feature/131503/1500_archers_on_a_288_network_.php.

[68] Shelton, Martin. "Signal, the secure messaging app: a guide for beginners." *Freedom of the Press Foundation*, 2 Feb. 2017, freedom.press/news/signal-beginners.

[69] Pash, Adam. "A beginner's guide to BitTorrent." *Lifehacker*, 3 Aug. 2007, lifehacker.com/285489/a-beginners-guide-to-bittorrent.

available for actual use.[70][71] The Signal developers themselves have gone on to conclude so much that it is impossible to fund an encrypted chat service without invalidating privacy by demanding users register with a phone number or without collecting metadata on their communications.[72] They also compain that they could not provide federation between a network of self-hosted servers owned and operated by the users, as this leads them naturally to congregating among a few popular servers that would take control over the entire federated network. Of course, this leaves Open Whisper Systems themselves in charge of the entire network instead. It is easy to imagine enough servers being distributed among the public as a shared commons that we could not become dependent on any singular group of system administrators controlling the network. It's not often you will find the CEO of a large company admitting this, but active development on the Matrix-Riot system of federated end-to-end encrypted communications challenges what Moxie has declared about the demands of the Signal protocol.[73]

Research from 2010 shows a purely client-to-client driven architecture would be infeasible for servicing a modern game on residential hardware[74], but bandwidth speeds are improving and other research showing a hybrid architecture[75] where some processing gets offloaded to clients already provides certain advantages. The immediate risks[76] posed by such an architecture that demand attention even in a network environment where available bandwidth meets the requirements are: loss of data and program state, inability for clients to join the network or to maintain stable connections, and cheating resulting from unvalidated client input. Centralized servers usually provide the resources to solve each one of these problems. Aaron Swartz, in the 2013 "A Programmable

[70] venomous0x. "WhatsAPI." *GitHub*, 3 May 2015, github.com/venomous0x/WhatsAPI.

[71] Enrico204. "Whatsapp-Desktop." *GitHub*, 27 Apr. 2018, github.com/Enrico204/Whatsapp-Desktop.

[72] moxie0. "Reflections: The ecosystem is moving." *Signal*, 10 May 2016, signal.org/blog/the-ecosystem-is-moving/.

[73] Hodgson, Matthew. "Matrix's 'Olm' End-to-end Encryption security assessment released - and implemented cross-platform on Riot at last!" *Matrix*, 21 Nov. 2016, matrix.org/blog/2016/11/21/matrixs-olm-end-to-end-encryption-security-assessment-released-and-implemented-cross-platform-on-riot-at-last/.

[74] Crowcroft, Jon and John L. Miller. "The Near-Term Feasibility of P2P MMOG's". *Proceeding NetGames '10*, 17 Nov. 2010.

[75] Chen, Alvin and Richard R. Muntz. "Peer Clustering: A Hybrid Approach to Distributed Virtual Environments." *Proceeding NetGames '06*, 31 Oct. 2006.

[76] Joshi, Rutvij, Swapna Naik, and Dharmik Patel. "Implementation of Peer-To-Peer Architecture in MMORPGs". International Journal of Science and Research, vol. 5, no. 10, Oct. 2016, pp. 1541-1546.

Web"[77], admits that, "Writing a social application so that it's peer-to-peer is about a thousand times harder than writing the same program as a web app." It would still, however, consist in the best method available to open up for public use, "…the freedom to modify how a program functions on our local computers as well as the ability to share and collaborate with others across the Internet." This type of research should serve as an open source guide for international groups to maintain communication within historically significant digital environments always at risk of sudden traumatic closure. Overall, while both p2p network architectures and properly encrypted systems introduce significant complexity in the design of programs that rely on each, it is becoming more readily conceivable to perform communications in this way based on available capabilities.

In "A Tale of Two Computers", Venkatesh Rao argues[78] that goal directed problem solving is an outdated feature of the geographic world and is not even compatible with the nature of the networked world in which problems instead get solved through tinkering by what he calls "serendipitous ways". This comes from the way tinkering generates, "…innovations that break assumptions about how resources can be used, typically making them less rivalrous and unexpectedly abundant." He claims that tinkerers perform the counter-intuitive but necessary social function of producing, "…access to as many people as possible," for resources that would otherwise either by individual or organizational interest be kept captive and idle.

Of course, bias could be shown to the group that manages to portray itself as the true inheritor of tinkering. Out of concern for this issue of the affirmation of so-called "white hat" hacking being potentially a rhetorical pretense, capture the flag hacking contests[79] are held throughout the year[80] between teams competing to break through specially designed encrypted systems made to test the players' skill at entering protected networks. Since the release of Edward Snowden's whistleblower data collected from NSA contractor Booze Allen Hamilton, the company has published a blog

[77] Swartz, Aaron. *A Programmable Web.* Morgan & Claypool, 2013, p. 48.

[78] Rao, Venkatesh. "Tinkering versus Goals." *Breaking Smart*, 1 Aug. 2015, breakingsmart.com/season-1/tinkering-versus-goals.

[79] Tangent, Dark. "DEF CON 26 CTF: Powered by The Order of the Overflow!" *DEF CON*, www.defcon.org/html/defcon-26/dc-26-ctf.html.

[80] Vittitoe, Steve. "How to Get Started in CTF." *Endgame*, 9 June 2014, www.endgame.com/blog/technical-blog/how-get-started-ctf.

post[81] advertising how its employees participate in CTF challenges they describe as a, "…high-stakes puzzle waiting to be solved, with real-world parallels that affect their work and all of our lives." These contests take place on closed-off dummy networks separate from the rest of the internet to prevent damages. The same techniques would apply so long as the game designers are employing state of the art, modern defenses in the systems they setup for players. Organizations that aim to tip the balance of encrypted systems in their own favor would not find themselves invulnerable to attack but would open up the grounds for another arms race to take over again. After leaving the company and fleeing the country, Snowden has gone on to say that all users should follow the rule: "Trust no one."[82]

A typical early pessimistic reading of video games had reduced them to the acting out of market economic forces of a pre-existing neoliberal order.[83] Even though we can clearly delineate types of economies internal to the structure of most video games, it is not at all clear there is any direct isomorphism between those and the real economy we find ourselves situated in, or for example where the general desire would come from for acting out these relations in a secondary imagined space besides that the games as commodity-objects may leave us implicit instructions for doing so. Studies of how people interact with games find them becoming hyper-attentive to specific details that would be glossed over in everyday affairs, leading to new emergent 'sandbox' exploratory types of behavior. Cheat codes and other game systems do not correspond to any kind of real abundance to be found freely within the limits of late capitalism, even while we are directed to believe that it has been over-accommodating to consumers by way of a system of social welfare absent any view of accompanying austerity measures. It bears repeating that games may end up continuing to serve as the obscene supplemental activity for those who spend the rest of their time engaged in work even with the military-industrial complex.[84]

[81] Allen, James and Brad Medairy. "Why Playing Capture the Flag Will Make You a Better Hacker." *Booze Allen Hamilton*, www.boozallen.com/e/culture/capture-the-flag.html.

[82] Samson, Ted. "Note to all Internet users: Trust no one." *InfoWorld*, 9 Jul. 2013, www.infoworld.com/article/2611303/note-to-all-internet-users–trust-no-one.html.

[83] Giddings, Seth. "Accursed Play: the economic imaginary of early game studies." *Games and Culture: a journal of interactive media*, vol. 13, iss. 7, 19 Feb. 2018, pp. 765–783.

[84] Kirkpatrick, Graeme, Kristensen, Lars, and Mazierska, Ewa. "Marxism and the computer game." *Journal of Gaming and Virtual Worlds*, vol. 8, no. 2, 2016.

Should it come as any surprise then, to find the president of the US staging war room photos of himself depicted next to his top generals exactly as he had previously observed his predecessor conducting such an actual meeting? This was done only without any of the ethernet cords laying on the table being plugged in - as though he considered it to be like a game.[85] Meanwhile, the Google DeepMind group is constantly enhancing its algorithms which "…answer questions about complex, structured data," by making machines consecutively replay through games over and over again until they encounter unpredicted routes that in their analysis produce new forms.[86] But what about when this same neural network gets turned back onto the problem of adapting encryption schemes against active adversaries assumed to be present on a network?[87] While the public has sometimes been able to maintain pace with private corporate algorithmic design, much of the advantage has come from bulk processing of data performed across many cumulative servers which has been more difficult for independent groups (besides for example, large universities) to sustain.

The political import of games has often been challenged so much as they present to us a space that is "not real", and so some theorists have argued that we should not take any fictional objects assumed to be encountered in those fictional spaces to be real. In "MMOG Ontology", self-described fictional realist Olav Asheim explores the premise that at least some fictional objects should not be taken to be real.[88] Instead, he shows how our ability to interact with machinery in the environment reveals "ludic" parts of the world that can still be held as real. This allows for counting or even logically quantifying over some fictional objects as being real corresponding exactly to how they enable these interactions. This experiment in design only consists in an open possibility and its outcome will be highly dependent on who will participate in facilitating games and whether they will be challenged[89] when allowed to consist merely in a virtual reproduction of the existing state

[85] Cockburn, Harry. "Anomalies in Trump situation room photo spark online conspiracy theories it was staged." *Independent*, 28 Oct. 2019, www.independent.co.uk/news/world/americas/us-politics/trump-al-baghdadi-dead-raid-syria-isis-photo-barack-obama-osama-bin-laden-a9174196.html.

[86] Graves, Alexander and Wayne, Greg. "Differentiable neural computers." *DeepMind*, 12 Oct. 2016, deepmind.com/blog/article/differentiable-neural-computers.

[87] Abadi, Martín and Anderson, David G. *Learning to Protect Communications with Adversarial Neural Cryptography*. arXiv preprint, 24 Oct. 2016, pp. 1-5.

[88] Asheim, Olav. "MMOG Ontology: How to be a Fictional Antirealist Ludic Realist." *The Philosophy of Computer Games Conference*, 2009.

[89] Bown, Alfie. *The Playstation Dreamworld*. Polity Press, 20 Nov. 2017, pp. 27-60.

of affairs. Steve Bannon, while not totally trustworthy, has admitted himself that his recruitment of lonely young men through massively multiplayer online games directly culminated in the vicious GamerGate movement.[90] Michael Prihoda, conversely, has used the game ReCore to reconfigure the expansive pioneering possibility space that corporate tech giants like Bezos and Musk present their visions as encompassing.[91] While the game holds a certain flaw in allowing an easy out to planetary climate collapse through the reactivation of a terraforming mechanism, it does not nearly match the realized failures of these men to contribute anything of significance to the development of human society on earth where almost every person must continue to find a way to survive for centuries to come.

In a speech given at *Game Developers Conference*, Chris King of Paradox has argued that one could take a broad overview of the military conquest history of a few of the great empires by playthroughs of multiple overlapping but qualitatively distinct games in the strategy genre, except that these have necessarily left out the highly exploitative stage of production involving colonial resource extraction.[92] In popular media depictions of social life, it has often been the case that both the exploitation and the inevitable cycles of general crisis are left out of the picture. It is only in the game *Victoria 2*, from 2010, that King finds he is able to explore something like an initial approach to this further complexity. He even makes an aside that Marx's theory of historical materialism would be good to follow for game developers, because like computer code it consists in a deterministic method.

This program will then involve the restoration and preservation of digital arts beyond the limited scope of their profitability, preemptive deterrents against excessive corporate litigation, and the delivery of encrypted traffic through high-speed, distributed p2p networks. This is done not for the cementation of a past but to ensure the examination of every aspect of a type of game so that

[90] Snider, Mike. "Steve Bannon learned to harness troll army from 'World of Warcraft'." *USA Today*, 18 Jul. 2017, www.usatoday.com/story/tech/talkingtech/2017/07/18/steve-bannon-learned-harness-troll-army-world-warcraft/489713001/.

[91] Prihoda, Michael. "ReCore: The Error in Misreading Dystopia". *Medium*, 28 Aug. 2018, medium.com/mammon-machine-zeal/recore-the-error-in-misreading-dystopia-81435d2af4e8.

[92] Campbell, Colin. "Karl Marx and the historical determinism of video games." *Polygon*, 18 Mar. 2016, www.polygon.com/2016/3/18/11264172/karl-marx-and-the-historical-determinism-of-video-games.

it can be included into the data to be used as the material for the construction of more complex forms. In the age of widespread general desktop computing, if there is no reasonable expectation of computer privacy every work will then serve an already pre-established public consensus. The non-disclosure of internally held information inflects the outcomes of playing games. Games present to us a space where not just one solution to a problem can be tested but virtually endless numbers of them contained within a specific ideological horizon given the same scenario is played out over and over again. For encryption, this means the best capabilities can be developed sparing considerations of cost-effectiveness and without breaking physical machines.