# VERIFIED, TRACKED, AND VISIBLE: A HISTORY OF THE CONFIGURATION OF THE INTERNET USER

by

CHRISTOPHER J. ST. LOUIS

A THESIS

Presented to the School of Journalism and Communication
and the Graduate School of the University of Oregon
in partial fulfillment of the requirements
for the degree of
Master of Science

September 2017

THESIS APPROVAL PAGE

Student: Christopher J. St. Louis

Title: Verified, Tracked, and Visible: A History of the Configuration of the Internet User

This thesis has been accepted and approved in partial fulfillment of the requirements for the Master of Science degree in the School of Journalism and Communication by:

| | |
|---|---|
| Peter Alilunas | Chairperson |
| Biswarup Sen | Member |
| Tara Fickle | Member |

and

| | |
|---|---|
| Sara D. Hodges | Interim Vice Provost and Dean of the Graduate School |

Original approval signatures are on file with the University of Oregon Graduate School.

Degree awarded September 2017.

THESIS ABSTRACT

Christopher J. St. Louis

Master of Science

School of Journalism and Communication

September 2017

Title: Verified, Tracked, and Visible: A History of the Configuration of the Internet User

The figure of the user is often overlooked in Internet histories, which frequently focus on larger treatments of infrastructure, governance, or major contributions of specific individuals. This thesis constructs a philosophical and ideological history of the Internet user and examines how that figure has changed though the evolution of the Internet. Beginning with the Web 2.0 paradigm in the early 2000s, a growing state and corporate interest in the Internet produced substantial changes to the structure and logic of the Internet that saw the user being placed increasingly at the periphery of online space as the object of state surveillance or behavioral tracking. The three case studies in this thesis investigate the combination of technological constraints and discursive strategies which have aided in shaping the contemporary user from active architect of the Internet itself to passive, ideal consumer of predetermined online experiences.

CURRICULUM VITAE

NAME OF AUTHOR: Christopher J. St. Louis

GRADUATE AND UNDERGRADUATE SCHOOLS ATTENDED:

University of Oregon, Eugene, OR
University of Tokyo, Bunkyo-ku, Tokyo, Japan
Southern Oregon University

DEGREES AWARDED:

Master of Science, Media Studies, 2017, University of Oregon
Master of Arts and Sciences, Information Studies, 2014, University of Tokyo
Bachelor of Arts, English, 2009, Southern Oregon University

AREAS OF SPECIAL INTEREST:

Internet Studies
Media Histories
Science and Technology Studies

PROFESSIONAL EXPERIENCE:

Daily Operations Manager, Inventure Inc., Jan. 2015 to Sept. 2015

Content Manager, QA and Customer Care Lead, Folium Partners Inc., Oct. 2010 to Apr. 2012

ACKNOWLEDGMENTS

I would like to thank my thesis committee members Drs. Biswarup Sen and Tara Fickle for their comments and advice when I was in the planning and proposal stages of this project, and especially for their detailed feedback towards future possibilities for this work at the defense. I am very grateful to my adviser and committee chair, Dr. Peter Alilunas, for helping to steer me through this whole project: for serving as a sounding board as I tried out new ideas, for encouraging me to stick with the good ideas when I had second thoughts, and for keeping me on track when the writing process threatened to overwhelm.

To Heather and Hazel, who continually reminded me why I was doing this when I had trouble remembering.

TABLE OF CONTENTS

Chapter Page

Chapter Page

# CHAPTER I

# INTRODUCTION: WHENCE THE INTERNET USER?

## Internet Histories

Histories of the Internet—and of personal computing in general—tend to approach their subject from one of two particular angles. The first is a focus primarily on the technological aspects: the protocols, standards, and physical advances which have enabled the ceaseless acceleration of information and communications technology over the past 60 years. The second angle is bibliographical, situating the technological within the lifespan and accomplishments of an important figure in the success of the Internet. The bibliographical works either restate known important contributions or attempt a sort of reclamation of the historical record by hitherto unknown figures; in either case, they take on a hagiographic note which writes the subject larger than life, representing it as an absolutely indispensable agent without whom computing today would not exist. Some of the most excellent histories—Janet Abbate's *Inventing the Internet* and Steven Levy's *Hackers: Heroes of the Computer Revolution* being two examples—are a mix of the two approaches, but very rarely do general histories have as their focus one of the most critical components to the success of the Internet, perhaps even more so than all of the technological advances: the figure of the user.

Users of the Internet, in the sense of various groups or communities, have been the subject of a number of ethnographic works: Julian Dibbell's *My Tiny Life*

takes a New Journalism-esque approach to the pre-Internet phenomenon of MUDs and MOOs ("multi-user dungeon," and "MUD, object-oriented," respectively), precursors to chat rooms that functioned something akin to a melding of text adventure games such as *Zork* and the roleplay of Dungeons & Dragons. Michael and Rhonda Hauben's *Netizens* examined both the technical and social development of USENET from a sort of poor-man's ARPANET mailing list to a global, decentralized discussion forum. Howard Rheingold's *The Virtual Community* explored the novel—in 1993—phenomenon of people congregating in online spaces such as the WELL (Whole Earth 'Lectronic Link) and IRC channels, forming communities akin to the ones which exist in the physical world. And Tom Boellstorff's *Coming of Age in Second Life* adopted established ethnographic practices from the physical world in examining the actions of users in the Second Life virtual world. But these research projects have all been constrained by the particular communities or technologies that they focus on and are generally fixed in a particular period of time—a detail made all the more obvious considering that many of these communities no longer exist or have been supplanted by current trends such as social media.

**Tracking the History of the User**

At the core of this thesis is the argument for a critical examination of the Internet user: a composite, abstracted figure which represents the prevailing ideology and technological constraints of the Internet in the particular era in which it exists. The Internet user—or more redundantly, the ideal Internet user—

is a reflection of the contemporary norms governing practices of online citizenship. Of course, the question must be asked: *whose* ideal Internet user? This is a definition which I will argue changes over the history of the user, according to the era; three such changes will be investigated in this thesis.

The Internet user in 1995, at the birth of the Internet, drew on a host of technological and conceptual predecessors. The jargon, attitudes, and history of the early LISP and then UNIX hackers; the mischievous network cartography of the boxers and phone phreaks; the communitarian ethics of early USENET residents and the technologically-savvy counterculture that took up residence in the WELL, all mixed together to produce a conceptual archetype born on April 30th, 1995: the Internet user. This user was consciously aware of its lineage and through the knowledge imparted by this history had considerable agency as both inhabitant and architect of the online space. But none of that would necessarily have been surprising: one was an Internet user because one *wanted* to be an Internet user. The network was limited in scope, difficult to connect to, and required specialized and expensive hardware that was not yet ubiquitous in computers—the diametrical opposite of the absolutely uninteresting nature of perpetual, invisible connectivity we take for granted today. The ideal of the Internet user in 1995 was recursively defined by the user itself, an identity informed by its past but actively created and refined as it was experienced.

The Internet user of today, by comparison, has little sense of its own subjectivity. With the ubiquity of the Internet in the developed world, to be a user

is much less of a conscious pursuit and something more akin to an active state of being. A 2014 American Community Survey report on computer and Internet use in the U.S. stated that almost three-quarters of American households (74%) have Internet access, and nearly each of those households has what is defined as high-speed access.[1] Compare this to 1997, two years after the Internet became publicly available, when only 18% of all households reported any sort of Internet access.[2] As with any technology that becomes so prevalent as to be taken for granted, the Internet today is entirely unremarkable. The proliferation of public Wi-Fi hotspots and high-speed home Internet access, the availability of low-priced laptops and netbooks, and the surge in mobile data access popularized by the release of Apple's iPhone in 2007 have all made accessing the Internet an entirely automatic and entirely boring process. Given this state of ubiquity, it's not surprising that the role of the user has shifted as well. No longer is the user required to be architect of their online experience, as the rapid commercialization of the Internet from the late 1990s onward has seen the broadly user-driven experience inverted into something driven by the advertising economy and arranged to extract the maximum value from the user as consumer/product. Advertising has become the dominant economic model online, and the structure of the web is designed to compel the user to participate most effectively in the cycle of targeted advertising that operates on the constant collection of user data. The ideal modern user, then,

1. Thom File and Camille Ryan, *Computer and Internet Use in the United States: 2013*, American Community Survey Reports (Washington, DC: U.S. Census Bureau, 2014), 3, accessed March 19, 2017, https://www.census.gov/content/dam/Census/library/publications/2014/acs/acs-28.pdf.

2. Ibid., 4.

is one that participates fully in the online advertising economy, in the dual role as diligent consumer who is marketed to, and as enthusiastic participant in the online experiences which collect the user's data for the production of more relevant targeted advertising.

**Defining "User"**

As always when undertaking research, it is imperative to define the terms to be addressed throughout the project. In this case, I wish to imbue the broad term "user" with a slightly more focused and specific meaning. I will be addressing a variation on the concept of the "end user," which the online *Merriam-Webster* dictionary defines as, "the ultimate consumer of a finished product."[3] The user operates a computer for work or leisure, and may indeed serve dual roles—through hobby interests or employment—as both a developer of consumer hardware or software as well as, by necessity, a user of those same technologies. More importantly, however, this definition of "user" must be located within a global and cultural context. Owing to the potential scope of attempting to theorize a universalized, global user and the time and resources required to adequately undertake such a project, my object of research will by necessity be limited to discussion of the user in the context of American computing culture and history. While this limited focus will regrettably exclude global experiences which reflect different technological traditions, it also ensures the feasibility of this work as a master's thesis. In the interest of brevity, I will refer to "the user" or "the

3. "End User," *Merriam-Webster.Com*, 2017, accessed August 30, 2017, https://www.merriam-webster.com/dictionary/end+user.

Internet user" throughout this thesis, but this designation should be taken to mean the Internet user in the American cultural and technological context.

## Case Studies

Throughout this thesis, I will argue that there has been a dramatic disenfranchisement of the Internet user from 1995 to today, corresponding both to the increasing commercialization of the Internet as well as the creeping expansion of the online surveillance state. The three case studies visited in this thesis highlight events which reflect the user's changing role as their agency is slowly reduced through constraints on technology and discursive construction of hegemonic social norms. The first case study concerns the online activation requirement of Microsoft's Windows XP operating system and its requirement of online verification of users under the justification of combating illegal copying. The second case study addresses the rise of online advertising in the Web 2.0 era and the transformation of the users into a commoditized audience, as well as one common practice of resistance to the advertising economy and how it is represented. Finally, the third case study looks at the disproportionate attention given to a small New Hampshire public library by national and state law enforcement following the library's participation in a project involving the Tor network, which allows users to browse the web anonymously. In each of these three cases, the events examined highlight the tension between the figure of the historically autonomous, engaged user, and the prevailing logic of the Internet that demands the user is always passive, verified, and visible.

This thesis will first attempt to define the figure of the Internet user circa 1995—not in demographic terms but in the sense of a broader theoretical genealogy—and will then map the relationship between the user and the changing ideological shape of the Internet in the following decades. This process will attempt to answer a few relatively broad questions: what does it mean to be "an Internet user" today Given the dramatic shift in agency that the user has undergone over the past 30 years, is it accurate to still include the Internet user of today in the same lineage as the one that emerged in 1995? Does even the word "user" imply a subjectivity that is no longer present, to the point where it would be inaccurate to talk about an "Internet user" today as distinct from any other form of consumer/audience?

The earliest narratives about the Internet—its creation myths, if you will, and the same ones that defined the heritage of the user—celebrated its democratic and emancipatory potential through a global connectivity and free sharing of information. These stories envisioned not so much the technology itself but a congregation of users all working cooperatively, facilitated through a conceptual medium that was "the Internet." But the user has been progressively subsumed under layers of state and corporate control, its potential for action limited to rigidly defined activities within a surveillant-capitalist framework, and it is certainly doubtful whether this retreating vision can ever become a reality, or whether it should be left in the 1990s with various other embarrassing exhibits of millennial techno-futurism. In theorizing the concept of "the Internet user,"

however, perhaps a new framework can be developed for identifying not only what has been lost in this transition, but practices of resistance which may ultimately assist the user in reclaiming its agency and realizing the democratic potential of the Internet.

# CHAPTER II

# LITERATURE REVIEW

## Introduction

In order to make an argument not only for the concept of "the Internet user" but that this figure has been subjected to substantial change over its history, we must first provide a definition of "the Internet user" as well as place it within its proper historical context. "The Internet user" as defined by this thesis refers not to a simple demographic quality but is instead a composite abstraction representing the cultural ideologies and practices of people using the Internet at a discrete point in time. A central aim of this thesis is to examine how this figure has changed over time in response to the possibilities offered by the changing shape of the Internet itself, while arguing that commercial structures and technological changes have made the Internet less centered around the user than it was at its inception. Correspondingly, the user possesses significantly less agency in actively shaping the structure of the Internet, a quality that arguably made the Internet as widespread as it is in the first place.

This chapter will first attempt to situate the figure of the Internet user within the lineage of computing culture which has come before. Starting from accounts of early hacker history, I will attempt to recreate an ideological and philosophical genealogy of the user which will have informed the shape of this figure at its inception in 1995. Next, this chapter will examine the drastic shift in ideology and economics known as Web 2.0 and its effect on the role of the user

online. The present Internet operates almost entirely according to a strongly capitalist logic, and Web 2.0 was the movement that ushered in this changed state. And finally, this chapter will engage with work from the field of surveillance studies as it applies to the present Internet. Surveillance studies has theorized the effects of surveillance on the body of the subject and its relationship to democratic society, but the context until very recently has general remained limited to theorizing the effects on the physical body under observation by the state. Recent works have attempted to re-contextualize familiar aspects of surveillance studies as applicable to online life, where the object of surveillance is not the production of more docile, predictable bodies in the service of the state, but rather the continued refinement of advertising processes that observe and capture increasingly detailed data on the user's online activities for the purposes of producing ever-more targeted forms of advertising. Here, the capitalist turn of Web 2.0 assumes its most distilled form, and the unwitting user is continually the subject of the advertising gaze while at the same time finding its potential activities online limited only to those conducive to advertising.

## Creating the User

The network culture wherein the user is situated owes a significant conceptual debt to a fusion of academic and counter-cultural traditions that preceded it. The Internet was officially "born" on April 30th, 1995, when the high-speed NSFNET backbone, run under a contract with the National Science Foundation that prohibited commercial or recreational use, was deactivated and

its network traffic switched over to the Internet proper, a parallel network infrastructure developed in cooperation by a number of major telecommunications companies.[1] We can consider the Internet user to have been officially "born" at this time, but technically the figure was simply the continuation of an existing paradigm, the inheritor of decades of received culture handed down from the first hackers.[2] Those histories form a sort of creation myth which informs, implicitly or explicitly, the ideological and philosophical character of the Internet user.

The origins of hacking culture emerge from the Tech Model Railroad Club at the Massachusetts Institute of Technology in 1958, as chronicled in Steven Levy's superb history of the topic. Technically-inclined students worked with great interest on the sophisticated electrical systems that controlled track switching, lights, and other infrastructural aspects of the TMRC's substantial model layout.[3] In 1959, MIT offered its first course in computer programming, which most of the technically-oriented TMRC members enthusiastically gravitated towards. Computer programming at that time was more akin to electrical engineering in practice, and the repurposed telephone equipment used in the switching systems

1. Janet Abbate, *Inventing the Internet* (Cambridge, MA: MIT Press, 2000), 198–199.

2. The term "hacker" is used in its original context as derived from the jargon/slang "to hack" as described in Levy, *Hackers* (9-10) and Guy L. Steele Jr. et al., "The Hacker's Dictionary," 1983, http://www.catb.org/jargon/oldversions/jarg150.txt, entry "HACKER." The negative connotations of the word produced by the news media are briefly discussed in Coleman, *Coding Freedom*, pps. 16-17.

3. Steven Levy, *Hackers: Heroes of the Computer Revolution* (Garden City, NY: Anchor Press/Doubleday, 1984), 7–9.

for the model train sets was not terribly removed from the innards which powered early computers.[4]

The TMRC culture was responsible for a significant amount of the jargon and wordplay still in use in hacking culture decades later: puns and witty substitutions such as swapping "orifice" for "office," lingo such as "cruft" (initially any accumulation of garbage or junk; its extant meaning refers to redundant or useless legacy code in a software program), and the timeless "hack," "a project undertaken or a product built not solely to fulfill some constructive goal, but with...wild pleasure taken in mere involvement."[5] This interplay between technical prowess and a clever, often irreverent engagement with the work itself, combined with a guild-like community spirit have since become well-known hallmarks of computing culture. A significant example of this, and a defining characteristic of computing cultures for decades to come, was the hacker ethic.

The "hacker ethic," in as much as it can be discussed in concrete terms, is a collection of values which accumulated in hacking culture as an unspoken guiding principle. Levy offers the following creed by way of explanation (though lacking any acceptable attribution): "access to computers—and anything which might teach you something about the way the world works—should be unlimited and total. Always yield to the Hands-On Imperative!"[6] This "hands-on imperative" is possibly more an invention of Levy himself than of the culture he surveys, but

4. Ibid., 11–12.

5. Ibid., 9.

6. Ibid., 27.

nonetheless reflects the almost instinctual hacker desire to tinker and see the inner workings of the object of fascination, be it a piece of computing hardware or a software program.

In an interview, Richard Stallman describes the hacker ethic at the MIT Artificial Intelligence Lab in the 1970s similarly, saying "hacking refers to the spirit of fun in which we were developing software. The hacker ethic refers to the feelings of right and wrong, to the ethical ideas this community of people had—that knowledge should be shared with other people who can benefit from it, and that important resources should be utilized rather than wasted."[7] As long as people had a legitimate desire to learn or work and would share the results of their work with other interested hackers, it seemed unethical to deny access to the necessary computing machinery. The situation at MIT at this time bordered on anarchic, with hackers treating such security measures as locked office doors as silly administrative impediments to the imperative of the hacker ethic. Stallman's biography offers a tongue-in-cheek appraisal of the dominant culture at the time: "if a faculty member made the mistake of locking away a terminal for the night, hackers were quick to correct the error."[8] The euphemistic way in which the situation is described—the faculty member "made the mistake" of locking their office with a valuable terminal inside, which was simply an "error" to be corrected

7. Richard Stallman, "Meme 2.04," interview by David S. Bennahum, Electronic newsletter, 1996, accessed July 30, 2017, http://memex.org/meme2-04.html.

8. Sam Williams, *Free as in Freedom: Richard Stallman's Crusade for Free Software* (Sebastopol, CA: O'Reilly Media, Inc., 2002), 48.

—offers insight into how strong the call of exploration was in the hacking culture of MIT.

Gabriella Coleman, however, argues that practices of hacking, especially relegated as it is today to a more subcultural area of mainstream computing, are much more nuanced than to be explained by a singular dogmatic creed, noting that "almost all academic and journalistic work on hackers commonly whitewashes these differences, and defines all hackers as sharing a singular 'hacker ethic'."[9] While acknowledging the fantastic historical value of Levy's *Hackers*, Coleman also notes that it was in this book—published in 1984—that the idea of a definitive "hacker ethic" became popularized. Approaching hacker culture from a more formal ethnographic mode of study, Coleman of course finds that sort of broad generalization implied in Levy's concept lacking acceptable nuance. But Levy is quick to point out the informal nature of this creed, saying that "the precepts of the revolutionary Hacker Ethic [sic] were not so much debated and discussed as silently agreed upon. No manifestos were issued. No missionaries tried to gather converts."[10]

As Coleman points out, there was indeed a manifesto of sorts issued, in a sense, on the ideals of the hacker ethic.[11] In 1983, Richard Stallman, a programmer at the MIT AI Lab, announced the creation of the GNU operating

9. E. Gabriella Coleman, *Coding Freedom: The Ethics and Aesthetics of Hacking* (Princeton, New Jersey: Princeton University Press, 2012), 17, http://gabriellacoleman.org/Coleman-Coding-Freedom.pdf.

10. Levy, *Hackers*, 26.

11. Coleman, *Coding Freedom*, 18.

system (for “GNU’s not UNIX,” an archetypal example of the pleasure of wordplay expressed in hacker culture)[12], an attempt at creating a “complete Unix-compatible software system which I am writing so that I can give it away free to everyone who can use it.”[13] Stallman was motivated to produce this operating system in response to the creeping advances of commercialization in the hacking world that foreshadowed the same developments on the web decades later. Researchers and employees at the AI Lab in the 1970s took it upon themselves to modify the software used on the Lab’s computing system to suit their needs, something that was possible at the time because the source code was freely available and free to redistribute. As Stallman described it, “whenever people from another university or a company wanted to port and use a program, we gladly let them. If you saw someone using an unfamiliar and interesting program, you could always ask to see the source code, so that you could read it, change it, or cannibalize parts of it to make a new program.”[14] This software sharing culture was an expression of any conscious ideology in the same way it exists today, but was instead simply a default cultural convention. However, Stallman noted an increasing number of incursions on that convention, all mounted by corporate entities with a vested interest in closing access to the inner workings of hardware. A Xerox printer donated to the Lab in 1980 was not accompanied by its source

12. Richard M. Stallman, “The GNU Operating System and the Free Software Movement,” in *Open Sources: Voices from the Open Source Revolution*, ed. Chris DiBona, Sam Ockman, and Mark Stone (Sebastopol, CA: O’Reilly Media, Inc., 1999), 32.

13. Richard M. Stallman, “The GNU Manifesto,” *GNU Project - Free Software Foundation*, last modified 1985, accessed August 1, 2017, https://www.gnu.org/gnu/manifesto.html.

14. Stallman, “The GNU Operating System and the Free Software Movement,” 31.

code, as Stallman learned when he attempted to modify the software that interfaced with the lab's networked computers to fix an issue of a recurring paper jam. Attempting to track down the source code, he was flatly told that it would not be provided to him and was locked behind a nondisclosure agreement, common practice today but the ultimate slap in the face in light of the neighborly culture of sharing that reigned up to that point at the lab.[15]

This saga of the printer features prominently in Stallman's own self-produced origin story, but it was just one in a series of events—the systematic hiring away of AI Lab programmers of the LISP Machine operating system by private corporations which sold competing (and closed-source) versions of the software, the replacement of the lab's computer terminals and server with new systems which did not allow the lab's hackers to make changes to the operating system—which inspired Stallman to create his own operating system that would maintain his philosophy of community and his vision of the hacker ethic.[16]

The central philosophical component of the GNU project was that it and all its component pieces would be what Stallman defined as "free software,"[17] a somewhat confusing term where the "free" refers not to price but to liberty. Free software grants to its users "four essential freedoms:" "The freedom to run the program as you wish, for any purpose," "the freedom to study how the program

15. Williams, *Free as in Freedom*, 4–9.

16. Ibid., 94–101.

17. "Free software" somewhat parallels the concept of open source software in that they both imply that the software is freely-modifiable thanks to the inclusion of the source code. Open source, however, does not imply the user freedoms granted by free software, and open source software may impose restrictions on the user's ability to modify and redistribute the source code.

works, and change it so it does your computing as you wish," "the freedom to redistribute copies so you can help your neighbor," and "the freedom to distribute copies of your modified versions to others. By doing this you can give the whole community a chance to benefit from your changes."[18] The four freedoms have since been codified in the GNU General Public License (GPL), a software license that uses copyright law to enforce the right to modify and share software which bears the license—a subversive technique colloquially known as "copyleft."[19] The GPL remains in strong use among free software and open source projects online, with some recent estimates indicating that over half of all software projects are released under terms of the GPL.[20] While Stallman and the GNU project ultimately have been overshadowed by the proprietary commercialization of computing, the persistence of the GPL and Stallman's philosophy have continued to inform the broader ideological leanings of more technically-inclined computer users, such as the ones first online in 1995.

**In the Virtual Community**

In 1996, less than a year after the birth of the Internet, the Telecommunications Act of 1996 was signed into law by President Bill Clinton. Ostensibly designed to reduce regulatory barriers to entry for companies interested in entering the telecommunications market or expanding from one area

18. Free Software Foundation, "What Is Free Software?," *GNU Project - Free Software Foundation*, accessed August 1, 2017, https://www.gnu.org/philosophy/free-sw.html.

19. Richard M. Stallman, *Free Software, Free Society: Selected Essays of Richard M. Stallman*, ed. Joshua Gay, 2nd ed. (Boston, MA: Free Software Foundation, 2010), 127.

20. Matt Asay, "GPLv3 Hits 50 Percent Adoption," *CNET*, last modified July 27, 2009, accessed August 6, 2017, https://www.cnet.com/news/gplv3-hits-50-percent-adoption/.

to another (for example, a telephone company expanding to provide cable television). In practice, it enabled a sort of reversal of preceding decades of monopoly breakups in the telecommunications industry by allowing a smaller number of large media companies to increasingly consolidate ownership of media channels and undercut competitors on price and content through ownership of the infrastructure.[21] In an impassioned (but certainly hyperbolic) moment, John Perry Barlow, former lyricist to the Grateful Dead turned cyber-activist as one of the co-founders of the Electronic Frontier Foundation, penned the revolutionary-minded "Declaration of the Independence of Cyberspace." It was a utopian screed that declared to "Governments of the Industrial World, you weary giants of flesh and steel…. You are not welcome here. You have no sovereignty where we gather."[22] In terms of actual effectiveness it was somewhat akin to a child informing the adults that they had no power in his clubhouse, but it represented a crucial moment in the evolution of the cultures that would have possibly the greatest effect on the become the Internet. Barlow represented a strand of cyberculture that had been on the verge of dying out since the Internet was opened for public—and commercial—use: the technological descendants of the hippies, who had congregated around online communities such as the WELL. The Internet was positioned as a space apart from "real world" politics, governed and

21. Jeffrey Layne Blevins, "Source Diversity after the Telecommunications Act of 1996: Media Oligarchs Begin to Colonize Cyberspace," *Television & New Media* 3, no. 1 (February 1, 2002): 97–101.

22. John Perry Barlow, "A Declaration of the Independence of Cyberspace," in *Crypto Anarchy, Cyberstates, and Pirate Utopias*, ed. Peter Ludlow (Cambridge, MA: MIT Press, 2001), 27–30.

regulated—to the extent that it *would* be regulated—according to its own internal logic.

This fierce sense of community and the demand to let it regulate itself has strong ties to formulations of community that existed in online spaces prior to the Internet. Julian Dibbell's *My Tiny Life* opens with the description of a house party that was overtaken by an evil clown named Mr. Bungle who, using a kind of voodoo doll, caused other party-goers to commit various indecent acts upon themselves and others in the vicinity. The conceit of Dibbell's narrative is that the entire book takes place within LambdaMOO, a text-based multi-user environment. Dibbell narrates a sort of community trial for the finally-captured Mr. Bungle in which he is finally expelled from the game, and while the author is more interested in making sure the reader shares his ironic amazement that these events are not actually happening in real life, what he unwittingly describes is a real community, with rules of conduct (formally codified or not), a democratized governing process, and users who have real, emotive relationships with the others.[23]

Howard Rheingold plays less a wide-eyed tourist and seems to genuinely be interested in the communities that he tours, and especially in the real-life relationships that develop behind the virtual interactions. A central theme that Rheingold continually returns to is that, while the relationships and interactions among members of these communities generally occur in a computer-mediated

23. Julian Dibbell, *My Tiny Life: Crime and Passion in a Virtual World* (New York, NY: Henry Holt & Company, 1998), 21–24.

environment, the interactions are no less real for it. Speaking at the funeral of a well-known WELL member who died of cancer yet carried on the interactions with the community until his death, Rheingold notes that "it's hard to sympathize with the charge that all online relationships are unreal when you've stood in front of a person's friends and family at their funeral."[24]

Michael and Rhonda Hauben are similarly evangelical about their virtual community of choice, the Usenet discussion board system, though they do focus more on the technical aspects of the system rather than specific personal connections. However, the history of Usenet probably gives us the most direct precursor to what the Internet was first like in 1995. Hauben and Hauben repeatedly note, in no uncertain terms, the democratized and user-centric nature of the technology, stating that "Usenet...is controlled by its audience. Usenet should be seen as a promising successor to other people's presses, such as the broadsides at the time of the American Revolution and the penny presses in England at the turn of the nineteenth century," and that "in its simplest form, Usenet represents democracy."[25]

At this point, we can see a conceptual framework for the concept of the Internet user start to emerge. Hacking traditions stretching all the way back to the Tech Model Railroad Club at MIT define a figure capable of and interested in shaping the technical world around it. Using the ideals of the hacker ethic and, as

24. Howard Rheingold, *The Virtual Community: Homesteading on the Electronic Frontier* (Cambridge, MA: MIT Press, 2000), 327.

25. Michael Hauben and Ronda Hauben, "The Social Forces Behind the Development of Usenet," *First Monday* 3, no. 7 (July 6, 1998), http://firstmonday.org/ojs/index.php/fm/article/view/609.

an example, the approach toward concepts of freedom and community described by Richard Stallman, we have the philosophical underpinnings for a user not simply engaged in the physical side of technology, but engaged in considering its actual and potential use in society. And the pre-Internet online communities described or defined by Barlow, Dibbel, Rheingold, and Hauben and Hauben suggest a social figure, participating in "social media" that existed before the common use of the term, each formulation being one that was entirely controlled by the users and shaped or managed according to their needs. These various details provide a broad but still complete theoretical formulation of speaking about "the Internet user," circa 1995—one of almost absolute agency online, and possessed of liberal and democratic ideals as to the shape and function of the Internet. This figure, however, would not remain indefinitely, and shortly after the Internet was opened to the public, it began to undergo change brought on by the new commercial ideologies that began to take root.

**Commodifying the User: Web 2.0 and the Californian Ideology**

The shift in status of the user from primary agent to commodity object has been gradual over the history of the Internet, and lacks any particular juncture that can be seen as a discrete beginning of this process. However, the drastic paradigm shift known as Web 2.0 is certainly a tangible point where these changes began to accelerate. Web 2.0 was a largely marketing-driven reconsideration of the Internet ecology as a whole: the nature of content, the increasing integration of big business, and the role of the user in the wake of the

dot-com crash of the early 2000s. The term was first popularized in 2005 by technology publisher and entrepreneur Tim O'Reilly at a conference for web developers and in a successive blog post, which has been—in something of a rarity for online sources of this type—perpetually enshrined in the archives of the O'Reilly Media website.[26] In attempting to delineate the difference between Web 2.0 and "Web 1.0" (more of a backronym than any kind of official designation), Cormode and Krishnamurthy note the following qualities:

> Web sites based on a particular set of technologies such as AJAX; Web sites which incorporate a strong social component, involving user profiles, friend links; Web sites which encourage user–generated content in the form of text, video, and photo postings along with comments, tags, and ratings; or just Web sites that have gained popularity in recent years and are subject to fevered speculations about valuations and IPO prospects.[27]

Placing particular web technologies such as AJAX[28] in the definition of Web 2.0 is a needless distraction, if not completely wrong; while these technologies are certainly important in the functioning of many Web 2.0 websites, they hardly help to describe and account for the significant shift in the relationship between the user, the corporate world, and the network itself. There is some disagreement that Web 2.0 even represents any sort of fundamental change in the functioning of the

---

26. Tim O'Reilly, "Design Patterns and Business Models for the Next Generation of Software," *O'Reilly Media*, last modified September 30, 2005, accessed May 2, 2017, http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html.

27Graham Cormode and Balachander Krishnamurthy, "Key Differences between Web 1.0 and Web 2.0," *First Monday* 13, no. 6 (April 25, 2008), accessed March 20, 2017, http://dx.doi.org/10.5210/fm.v13i6.2125.

28. Asynchronous JavaScript and XML, a technology that allows a webpage to provide a certain amount of interactivity client-side, without having to send data back to the web server. For the original description and definition, see Jesse James Garrett, "Ajax: A New Approach to Web Applications," *Adaptive Path*, https://web.archive.org/web/20080702075113/http://www.adaptivepath.com/ideas/essays/archives/000385.php.

network: Allen rightly notes that "[Web 2.0's] distinctive assertion of a change in state, from Web 1.0 (a term that was never used in any case) to Web 2.0, begs the question of the degree to which this change has actually occurred or may be occurring because of something new, or simply involves a re–expression of things previously understood as 'the Web', but placed in a new arrangement or seen in a new light."[29] Scholz similarly states that "Web 2.0 is a good example of marketers entering the discussion about the Internet."[30] Perhaps more importantly than disagreements on nomenclature, Scholz continues to note that many of the concepts central to Web 2.0—the primacy of user submitted content in wikis, blogs, and other types of sites; publication formats such as RSS, and concepts such as the collective intelligence that accompanies the social diffusion of information online—have all existed in relatively unchanged forms in previous decades, and it is only the convergence of these concepts and technologies that is in any way remarkable.[31] Whether or not Web 2.0 was an actual, quantifiable change in the Internet is almost irrelevant—more so than any substantive technological advance, the dramatic shift in the role and value of the user is its lasting legacy.

The power dynamics of online spaces too have changed; while early Internet culture and structure inherited and was defined by the meshing of

29. Matthew Allen, "Web 2.0: An Argument against Convergence," *First Monday* 13, no. 3 (2008), accessed May 1, 2017, http://firstmonday.org/ojs/index.php/fm/article/view/2139.

30Trebor Scholz, "Market Ideology and the Myths of Web 2.0," *First Monday* 13, no. 3 (March 3, 2008), accessed March 20, 2017, http://dx.doi.org/10.5210/fm.v13i3.2138.

31. Ibid.

anarcho-libertarian and post-hippie ideologies, Web 2.0 saw a massive influx of corporate influence on the structure of the Internet that brought the network under the control of a new but entirely natural-seeming capitalist logic.[32] Barbrook and Cameron call this the "Californian Ideology," a new cultural chimera that "simultaneously reflects the disciplines of market economics and the freedoms of hippie artisanship."[33]

Prior to the Internet, the users were instrumental in the development of early networks, where participation in online life meant contributing to the shape of the network itself. Fundamental components of the modern Internet including email, bulletin board systems, and even the World Wide Web, the paradigm through which the Internet is most commonly experienced, were produced by users seeking to refine the network experience.[34] Jonathan Zittrain calls this quality "generativity," or the property by which a computing system has few artificial limits on its potential from the manufacturer, and is free for the user to customize as they see fit. This is being replaced by an *appliancized* model, referred to also as the "walled gardens" that curate an experience for the user at the expense of autonomy.[35] These curated experiences mean that the users are

32. Katharine Sarikakis, "Ideology and Policy: Notes on the Shaping of the Internet," *First Monday* 9, no. 8 (August 2, 2004), accessed April 12, 2017, http://dx.doi.org/10.5210/fm.v9i8.1167.

33. Richard Barbrook and Andy Cameron, "The Californian Ideology," *Science as Culture* 6, no. 1 (January 1, 1996): 50.

34. Manuel Castells, *The Internet Galaxy: Reflections on the Internet, Business, and Society* (Oxford, UK: Oxford University Press, 2002).

35. Jonathan Zittrain, *The Future of the Internet--And How to Stop It* (New Haven, CT: Yale University Press, 2008).

handing over control of their Internet experience to the producers of the walled garden. In giving up this control, the average user is also implicitly accepting and subjecting themselves to the politics that govern the walled gardens they experience.

## Watching the User: Surveillance Capitalism and the Post-User Internet

Langdon Winner questions the general assumption that technological artifacts—a computer, an operating system, a network—are inherently apolitical, pure and divorced from human influence or bias, in relating the history of the city planning of Long Island, New York in the middle of the 20th century. The city planner designed overpasses above roads to be far too low to allow for most commercial traffic to pass—including public buses. The poor and immigrant populations who relied on public transportation were effectively excluded from these neighborhoods and separated from the wealthy white citizens who lived there.[36] In this way, the racist ideology of the city's master planner was reflected in the very architecture of the city. This was a regulation of the movement of physical bodies that did not actually derive its power from juridical actions: the ideologies of racism and classism were embodied in the artifact itself.

Lawrence Lessig famously declared that "code is law," which adapts the politics of artifacts for the information age.[37] The design of a technical system

36. Langdon Winner, "Do Artifacts Have Politics?," *Daedalus* 109, no. 1 (1980): 121–136.

37. Lawrence Lessig, *Code: And Other Laws of Cyberspace, Version 2.0* (New York: Basic Books, 2006).

functions as something akin to a legal framework in the way it constrains the possible actions of the user. In a similar fashion, the politics of the Californian Ideology are reflected in—and become the de facto governing logic of—the non-generative Internet. Robert Gehl notes that users are compelled through the interfaces of Web 2.0 that encourage production and sharing of creative works, and especially through the formations of social media networks, to function as "affective processors," producing valuable data through taking part in the social net. Terranova notes that this annexation of the user's labor "is not about capital descending on authentic culture but a more immanent process of channeling of collective labor (even as cultural labor) into monetary flows and its structuration within capitalist business practices."[38] Gehl notes that, for all the discursive attempts at situating the user in the center of the Web 2.0 internet, true power online lies with the owners of Web 2.0 websites, who "surveil every action of users, store the resulting data, protect it via artificial barriers such as intellectual property, and mine it for profit."[39]

When Haggerty and Ball theorized the surveillant assemblage as the ultimate concatenation of formerly discrete systems of surveillance through new digital technologies,[40] they could not have anticipated the ease with which such a system could actually be put into practice online. One critical difference is that in

38. Tiziana Terranova, *Network Culture: Politics for the Information Age* (London: Pluto Press, 2004), 80.

39. Robert W. Gehl, "The Archive and the Processor: The Internal Logic of Web 2.0," *New Media & Society* 13, no. 8 (December 2011): 1228–1244.

40. Kevin D. Haggerty and Richard V. Ericson, "The Surveillant Assemblage," *The British Journal of Sociology* 51, no. 4 (December 1, 2000): 605–622.

most literature of surveillance studies, the surveilling agent is often assumed to be, if only implicitly, the state. Here instead the user is constantly monitored by website owners in what Shoshanna Zuboff terms "surveillance capitalism." The ultimate intent of corporate surveillance in the network is not the disciplined bodies of state governmentality, but production of value from the very presence of the user itself: "subjectivities are converted into objects that repurpose the subjective for commodification."[41] This is what David Lyon referred to as the data double, "various concatenations of personal data that, like it or not, represent 'you' within the bureaucracy of the network."[42] Once again, the assumed state bureaucracy is actually replaced with the machinery of surveillance capitalism, and the data double is used not in the production of docile bodies[43] but as an object of monetary value in its own right.

To this end, the structure of the Internet itself—the *politics* of a Web produced by the Californian Ideology, dictate the agency afforded to the user/product. The user is continually tracked as they move through the network, and access to some spaces is conditional on the information that the user volunteers. Terms of service and privacy polices which govern the user's acceptable interaction with the websites they visit, and which outline the way in which the user's personal data is collected, stored, and sold are unilateral, offering

41. Shoshana Zuboff, "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization," *Journal of Information Technology* 30, no. 1 (2015): 75–89.

42. David Lyon, *The Electronic Eye* (Minneapolis, MN: University of Minnesota Press, 1994).

43. Michel Foucault, *Discipline & Punish: The Birth of the Prison* (New York, NY: Vintage Books, 1977).

no potential of the user's negotiating the terms and which read continued use of the site as implicit consent that the user agrees to the terms. Surveillance is constant; the user's activity is continually monitored so that the network can ultimately redirect a wayward user into a more sanctioned mode of browsing.

## Conclusion

This chapter first began to produce a rough genealogical framework for theorizing the figure of the Internet user, based on histories of cultures and philosophies that existed before it. Next, this chapter examined the ideological foundations of the Internet's movement to Web 2.0, which possibly had the greatest effect in beginning to reshape the Internet into a form that no longer features the user as the central agent. And finally, theoretical aspect of surveillance and the meshing of surveillance and capitalism online provide us with a foundation for the current logic of the Internet, where the user is subjected to a continual surveillant gaze by both the state as well as commercial entities.

The following case studies will attempt to build a case for the transformation of the user in these three contexts above. The first case study, concerning mandatory online activation of the Windows XP operating system, sees the user given less control over the technical aspects of the world around them as they are required to prove their identity—in this case, as the legitimate owner of a software program—to an external party. The second case study follows the development of advertising and the user's shift to an audience commodity in a web where they no longer are given free range of movement that is not tracked

and reduced to a commodity value. And the final case study concerns technologies which allow the user to resist the directive that they always remain tracked and visible, though this activity is outside of prescribed behavior for the user and is not without consequences.

# CHAPTER III

# METHODOLOGY

## Reading Internet Histories

Both the preceding review of literature as well as the case studies to follow this chapter are concerned with the reading of what can generally be called Internet histories. This thesis itself aims to situate these histories within a broader historiography that argues for a figure of "the Internet user" and attempts to chart its genealogy over the past three decades as a means to investigate and critique the shape of the Internet itself, which has until recently been inseparably linked to the figure of the user.

The histories that comprise my reference materials span a broad range of the written medium, including a significant number of transient, digital sources such as blog posts, pages on corporate websites, plain text files, etc. These sources all provide a snapshot in time of online life and call back to past discourses that have affected online cultures represented in the writings. In addition, that these sources also often respond—explicitly or otherwise—to contemporary trends which have the potential to shape the Internet in a way that is not always aligned to the interests of the users. This chapter will outline the methods used in collecting and compiling the documents that represent these narratives as well as the methods used in analyzing this body of knowledge and identifying the discursive formations produced therein.

## Web Sources and Archival Problems

In the collection of textual sources for the case studies, I will use a broad historical approach that draws from media and mass communication research methods, document analysis, and somewhat theories of web historiography. The online sources I use are important as they provide an immediate record of or reaction to the specific events that serve as the main focus of the chapters, but they also present unique challenges. The web itself is not intended as an archival medium, and while it is possible for webpages to remain untouched for decades, it is far more common to encounter pages with missing content, broken links, or which have vanished completely. Websites can provide a significant contribution to the historical record, but are also subject to problems of completeness and accuracy that in the context of more formal archives of historical documents would be considered unacceptable.

John Scott describes four properties by which historical documents should be evaluated: authenticity, credibility, representativeness, and meaning. These properties are all concerned with establishing initial authorship and fidelity of reproduction of the documents; whether the documents are an accurate and genuine representation of events depicted; whether the documents constitute a representative sample (which necessitates the survival and availability of related documents); and the ability of the researcher to interpret meaning from the document contents.[1] While the interpretation of content in web sources poses no

1. John Scott, *A Matter of Record: Documentary Sources in Social Research* (Cambridge, UK: Polity Press, 1990), 18–28.

particular challenges unique to the medium, the transitory nature of web-based sources makes establishing authenticity, credibility, and representativeness difficult.

Megan Sapnar Ankerson addresses a unique problem that emerges with web-based sources, noting that "unlike paper or DVDs, which can be saved in their original form of presentation, saving web content demands action."[2] Whereas other forms of both print and electronic media are fixed into a physical—and therefore easily archived—form by the process of their publication, online sources must intentionally be saved to a reproducible format to guarantee future availability. Within the context of online sources, content from the initial ("Web 1.0") era of the Internet and the later Web 2.0 paradigm each pose their own specific problems with regard to long-term availability. As pre-Web 2.0 websites were largely static, HTML-based pages, it is unlikely that the content itself will have changed for any extant sites—assuming they still exist. Old websites of this particular geological strata are often unceremoniously abandoned, either at the individual level or on a massive scale, as was the case of GeoCities, a website owned by Yahoo which provided free website hosting and was one of the most-visited websites of the early Internet. Citing declining traffic, Yahoo opted to close the site in 2009 and gave its users a brief window in which they could back up their hosted data.[3] Given the age of the service, many of the websites it hosted

2. Megan Sapnar Ankerson, "Writing Web Histories with an Eye on the Analog Past," *New Media & Society* 14, no. 3 (May 1, 2012): 387.

3. Leena Rao, "Yahoo Quietly Pulls The Plug On Geocities," *TechCrunch*, April 23, 2009, accessed June 28, 2017, http://social.techcrunch.com/2009/04/23/yahoo-quietly-pulls-the-plug-on-geocities/.

were no longer maintained by their creators at the time of the closing, meaning that any data on the sites was unlikely to have been rescued and reproduced (or mirrored) in a newer location.

The ideology of Web 2.0, however, has a particularly problematic effect on historical research as it places an emphasis on what Tim O'Reilly called "the perpetual beta," or the fact that web content today rarely remains static for long.[4] With a near-zero cost of publication compared to offline media, information on modern websites is rapidly overwritten, revised, or relocated and primary sources can and do disappear completely, creating broken links that now point to empty spaces where a page once existed. And not only primary sources are affected by these changes: a website linking to primary information hosted elsewhere must either assume that the content it links to is permanent (and risk ending up with broken links when the linked content is eventually deleted or moved), or it must take an active approach to mirroring or archiving important linked content, which would effectively transform the primary source into a secondary one.[5] A third approach lies in the production of archived versions through automated processes, which is the most effective method to date of ensuring data on the web does not simply vanish, but which also poses additional problems in terms of the fidelity of the reproduction.

---

4. Tim O'Reilly, "Design Patterns and Business Models for the Next Generation of Software," *O'Reilly Media*, last modified September 30, 2005, accessed May 2, 2017, http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html.

5. This approach comes with a number of practical concerns, such as the storage space and bandwith necessary for reproducing the mirrored content, as well as copyright issues that may arise from hosting content without the permission of the creator.

One of the most common means of archiving web content is the use of programs that crawl the Internet and cache existing versions of pages, producing a snapshot of the page as it existed at that point in time. The Internet Archive is an organization dedicated to the preservation of web history, and its Wayback Machine utility represents the most comprehensive and accessible web archiving project, claiming over 286 billion webpages saved at the time of this writing.[6] A user visiting the archive can enter the URL of a website and view all cached versions of the site. In some cases, this is the only way to access information contained in deleted websites or pages, especially those from the pre-Web 2.0 era. For example, the entirety of the content on GeoCities—at least, what was still available in 2009—is retained in a special collection on the Internet Archive, following an initiative to save as many of the pages as possible before GeoCities finally closed.[7]

Automated archiving processes are not perfect; in addition to honoring the wishes of website owners who request that their webpages not be archived, the Wayback Machine has difficulties accurately capturing certain types of linked or dynamic content. Ankerson notes that "rarely are the contents of a site preserved and the 'snapshots' are often incomplete with missing images and broken links," and that the automated software sometimes attempts to fill in missing content (particularly images) with a best-guess approach that substitutes images from

6. "Internet Archive: Wayback Machine," accessed June 29, 2017, https://archive.org/web/.

7. "GeoCities Special Collection 2009," *Internet Archive*, accessed June 28, 2017, https://archive.org/web/geocities.php.

different historical versions of the same website, or which match the expected name and file type of the missing content.[8] But rather than treat these sources as secondary, incomplete, or inauthentic, Niels Brügger argues that "the process of archiving creates a unique version, but not a copy" of material online.[9] This approach however poses problems according to Scott's rubric of authenticity; if an archived copy is the only remaining version of a website, is it impossible to verify that it is an accurate reproduction of the original content and that errors have not been introduced in the archival process. Using websites as primary sources requires acknowledging the nature of web archiving and treating the archived website as a proper historical document in its own right, rather than a damaged and incomplete referent to a possibly-lost primary source. Keeping in mind these limitations, I will rely heavily on archived copies of websites saved through the Internet Archive to obtain credible—though not completely authentic—copies of texts where extant versions no longer exist in the open web.

## Discourses of the User

The sources used in this thesis all contribute to the production of discourses about the figure of the user, represented in two broad categories. The first category is engaged in what Gabriella Coleman calls "self-directed cultural representation,"[10] or discourses produced by and about the users themselves in a

8. Ankerson, "Writing Web Histories with an Eye on the Analog Past," 386.

9. Niels Brügger, "Website History and the Website as an Object of Study," *New Media & Society* 11, no. 1–2 (February 1, 2009): 127.

10. E. Gabriella Coleman, *Coding Freedom: The Ethics and Aesthetics of Hacking* (Princeton, New Jersey: Princeton University Press, 2012), 17, http://gabriellacoleman.org/Coleman-Coding-Freedom.pdf.

sort of auto-ethnography. The second category of discourses is produced by external actors—the software companies, website owners, and the advertising corporations that have increasingly come to dominate the web's ecosystem. This second type of discourse works to compel the user to a normative mode of online behavior most beneficial to these actors. Moving chronologically through the following case studies, there is a growing tension between these two categories of discourse, with the external economic discourses exerting stronger control over the ways in which the user is constituted while the self-reflexive discourses of the user occupy an increasingly niche cultural space online.

The discourses in the case studies serve an ideological function—as all discourse does, in some way—in reproducing the ideas of the dominant class, presented as a "natural" or "universal" order of things which may not actually be either as natural nor as universal as they seem.[11] Norman Fairclough emphasizes the practical and visible ways in which discourses reflect systems of power and control, noting that "the way in which orders of discourse are structured, and the ideologies which they embody, are determined by relationships of power in particular social institutions, and in society as a whole."[12] The discourses investigated here all operate in a constant re-articulation of the neoliberal Californian ideology that is the defining hegemonic logic of the modern Internet. Fairclough speaks of discourse as "the power to constrain *content*: to favor certain

11. Norman Fairclough, *Language and Power*, Language in Social Life (New York, NY: Longman, Inc., 1989), 33.

12. Ibid., 31.

interpretations and 'wording' of events, while excluding others."[13] There is an aspect of Althusserian interpellation at work here as well, as these discourses actively reaffirm the position and status of the individual user within the structure of post-Web 2.0 Internet. The user that accepts the terms of access and use online without complaint and is always willing to be verified—in other words, the user that participates in the Internet economy as intended—is the ideal user and a good online citizen. The user becomes criminal, deviant, when they sink to the level of the pirate, or when they actively violate the social contract that dictates their acceptable use of and interaction with websites.

Critical discourse analysis seeks to make visible the hidden workings of power within discourse that has become naturalized or is otherwise taken to be "common sense."[14] By employing critical discourse analysis in the following case studies, I intend to call attention to the ways in which the discourses surrounding these three historical events online have all worked to redefine the discursive formation of the ideal Internet user. The normalization of these discourses, and the acceptance of their ideological foundations as the natural order of online life not only serves to prescribe acceptable behavior for the disciplined user, but firmly rejects, opposes, and criminalizes the possibility of any users existing outside of—or worse, in resistance to—the dominant capitalist order.

13. Ibid., 52.

14. Norman Fairclough, *Critical Discourse Analysis: The Critical Study of Language*, Language in Social Life (New York, NY: Longman, Publishing, 1995), 28.

# CHAPTER IV

# CASE STUDY I: THE USER IS VERIFIED—AUTHENTICATING LEGITIMATE USERS UNDER MICROSOFT WINDOWS XP

## Introduction

Microsoft's Windows XP operating system was released in October 2001 and was the most-used operating system in the world for about ten years, until it was eclipsed by the later Windows 7.[1] The OS was actively supported for nearly 14 years until it finally reached end-of-life in April 2014,[2] making it the longest-lived Microsoft operating system ever released. While Microsoft has not released concrete sales figures, most estimates place the total number of copies sold in this time period at well above 500 million.[3] But aside from its longevity and significant legacy, Windows XP also represented a drastic change in the relationship between operating system and user that would help set a precedent for future concepts of software ownership.

The release of Windows XP was accompanied by substantial hype and a sophisticated marketing campaign which included a full-scale celebration in Times

1. Kate Solomon, "Windows 7 Use Finally Overtakes Windows XP," *TechRadar*, last modified October 17, 2011, accessed May 7, 2017, http://www.techradar.com/news/computing/pc/windows-7-use-finally-overtakes-windows-xp-1034482.

2. Microsoft Corporation, "Support for Windows XP Ended," *Windows XP End of Support*, last modified April 8, 2014, accessed May 7, 2017, https://www.microsoft.com/en-us/WindowsForBusiness/end-of-xp-support.

3. Desire Athow, "Windows XP End-of-Life: Thanks for All the Fish!," *TechRadar*, last modified April 6, 2014, accessed May 7, 2017, http://www.techradar.com/news/software/operating-systems/windows-xp-end-of-life-what-you-need-to-know-1240791.

Square,[4] featured the use of a hit single from Madonna's most recent album,[5] and which was projected to cost the company around one billion dollars.[6] While Microsoft had previously attempted to make releases of its operating system into pop-culture events—the company licensed a Rolling Stones song for Windows 95 promotional materials[7] and selected ambient composer Brian Eno to produce the signature startup sound for the OS[8]—the extent to which Microsoft promoted the XP launch suggested a change in the way future software and hardware would be announced and released. This attempt at making an operating system feel more like an *experience* rather than simply a functional tool was part of an accelerating trend. From gaming console launch parties played by superstar DJs to Steve Jobs' iconic product announcements at Apple's Worldwide Developer Conferences (especially the signature "and there's one more thing," which preceded a major product reveal and predictably drew the gathered faithful into ecstatic applause) computing technology in general was in the process of being reframed as

4. Tobi Elkin, "Glitzy Times Square Debut for Windows XP," *Ad Age*, October 25, 2001, accessed August 4, 2017, http://adage.com/article/digital/glitzy-times-square-debut-windows-xp/33069/.

5. Associated Press, "Microsoft Campaign Borrows Madonna's 'Ray,'" *Billboard*, last modified October 16, 2001, accessed June 30, 2017, http://www.billboard.com/articles/news/78081/microsoft-campaign-borrows-madonnas-ray.

6. Joe Wilcox, "Windows XP Marketing Tab to Hit $1 Billion," *CNET*, last modified June 26, 2001, accessed June 30, 2017, https://web.archive.org/web/20140201144711/http://news.cnet.com/2100-1001-269032.html.

7. Joe Wilcox, "Microsoft Readies XP for Late October," *CNET News.Com*, last modified May 9, 2001, accessed June 30, 2017, https://web.archive.org/web/20011130011654/http://news.cnet.com/news/0-1003-200-5870654.html.

8. Joel Selvin, "Q and A With Brian Eno," *SFGate*, last modified June 2, 1996, accessed June 30, 2017, http://www.sfgate.com/music/popquiz/article/Q-and-A-With-Brian-Eno-2979740.php.

something simple and approachable. Cryptic commands and jargon, text-interfaces which may as well have been written in an alien language, and even the pop-cultural shorthand image of the bearded, disheveled computer guru gave way to technology sealed behind sleek exteriors and intuitive interfaces that one could actually look cool while using. No longer was the power of the technology going to be reserved only for those who knew the proper incantations.

One consequence of this paradigm shift is a foundational problem that lies at the core of this entire thesis: that as information technology became infinitely easier to access, the technical complexity that granted the user control over these devices and programs was simultaneously abstracted and obscured. The inner workings of software and hardware were not things the end user wanted to concern themselves with, the reasoning went—but also, that they had no *need* to concern themselves with. The idea of control in the context this era of computing was seen as a zero-sum game: the more control given to the user, the less control the software's creator has over its use, and vice-versa. When control becomes disproportionately situated in the hands of the creator—under narratives of 'wanting to provide the best user experience' or 'to guarantee the stability of the software', etc.—the creator then is able to dictate terms by which the user can participate in its experience. In the case of Windows XP, this means that Microsoft was able to insist, for the first time, on conditions of using its software that extended beyond simple technical requirements: namely, that any user of Windows XP was to be verified.

## The History of Windows Product Activation

In addition to the cultural shifts described above, Windows XP represented a significant technical break from previous versions of the operating system. Windows previously was developed in two parallel lineages: the consumer-oriented Windows 9x line built on old MS-DOS technology that included Windows 95, 98, and ME, and the business/server-oriented Windows NT platform.[9] With Windows XP, all future releases of Windows would be built on the NT kernel, meaning that consumer products would share the same codebase as the server-oriented releases, a move which brought much-needed stability to the notoriously buggy consumer line. Over its lifespan, Windows XP would come to see support for a number of now-ubiquitous computing technologies such as Bluetooth, USB, and WiFi. But the changes most relevant to the discussion here were the ones made to Microsoft's Product Activation technology.

Starting with Windows 95, each version of the operating system required the use of a product key—referred to by Microsoft as the proper noun "Product Key"—during installation to verify that the installed software was not illegally copied. In an archived version of the section of its website dedicated to discussion of illegal copying countermeasures, Microsoft noted that "the goal of Product Activation is to reduce a form of piracy known as 'casual copying' or 'softlifting'."[10]

9. Stephanie Miles, "Microsoft Consolidates Windows Development Efforts," *CNET News*, January 24, 2000, accessed August 4, 2017, https://web.archive.org/web/20121107235539/http://news.cnet.com/Microsoft-consolidates-Windows-development-efforts/2100-1040_3-236021.html.

10. Microsoft Corporation, "Microsoft Piracy - Piracy Basics," *Protecting Against Software Piracy*, last modified June 9, 2001, accessed October 22, 2016, https://web.archive.org/web/20010609221208/http://www.microsoft.com/piracy/basics/xp_activation.asp.

While these particular terms don't seem to be used outside of the Microsoft corporate context, the larger point is that the use of a product key and associated technologies is designed to prevent noncommercial sharing of Microsoft software at the level of individual users. Microsoft is generally less forthcoming about its efforts at halting large-scale, commercial counterfeiting more befitting of the label "piracy," but an earlier archived version of its software piracy page describes features such as holograms, heat-sensitive ink, and textured printing used in the Certificates of Authenticity [sic] that accompany Microsoft products.[11] These features mirror anti-counterfeiting measures used in paper currency, and presumably function in a similar manner by allowing law enforcement to identify channels through which counterfeit software is produced or sold. But the greater concern, as suggested by the larger amount of website real-estate devoted to the topic, is the sharing of software between users. In its 2001 explanation of Product Activation technology, Microsoft states that "[casual copying] has been estimated by some industry trade groups to account for a staggering 50 percent of the economic losses due to piracy. Worldwide, the piracy rate is estimated to be 37 percent."[12] As with most corporate-produced reports and whitepapers on the topic of illegal software copying, the sources for these figures are never cited, and it may not be unreasonable to assume that the nearly 1-in-3 figure for worldwide

11. Microsoft Corporation, "What Microsoft Is Doing About Piracy," *Microsoft Protection Against Software Piracy*, last modified 1998, accessed July 1, 2017, https://web.archive.org/web/19990429132907/http://microsoft.com:80/piracy/microsoft/default.htm.

12. Microsoft Corporation, "Microsoft Piracy - Piracy Basics."

infringement takes the disingenuous route of combining occurrences of 'casual copying' with those for commercial counterfeiting.

The use of a Product Key on the Windows 9x series of operating systems was certainly not an unusual practice in the late 1990s. Product keys, also called CD keys, often accompanied software (especially games), and required that the user have not only the physical medium that the software was stored on, but also the manual, certificate of authenticity, or other document which provided the CD key. Presumably, only the legitimate owner of an original copy of a software program would possess the accompanying documentation. But very rarely did these protection practices extend beyond a localized verification of an authentic CD key—online CD key checking was uncommon, largely limited to the realm of online multiplayer games to ensure that multiple players were not sharing the same CD key.[13] In the case of Windows, the Product Key was an alphanumeric string that varied in length depending on the version of the OS, and was found on the Certificate of Authenticity which accompanied the operating system disc. For computers purchased with Windows preinstalled, the product key was located on a sticker on the case. The operating system checked the key for authenticity during the installation process and, if the key was found to be genuine, the operating system was legitimate and the installation process would be allowed to commence. Invalid keys would simply prevent the installation from completing.

13. Perhaps the best example of this is the Battle.net online service from Blizzard Entertainment, creator of the *Diablo*, *Starcraft*, and *Warcraft* series. Blizzard implemented a CD key check—for online play only—through Battle.net in 1998 with the release of *Starcraft*. See http://classic.battle.net/info/faq.shtml.

But given that the product keys were verified by the operating system and there was no way to ensure that a single key was used for only one installation, the overall effectiveness of the activation process was compromised from the beginning. A user could simply share one copy of the Windows software among multiple computers, or multiple users could share the same copy of the software between them. Programs known as “keygens” (from “key generator”) circulated freely online. These programs either functioned as the name implied and mathematically generated a product key that would be approved by the operating system’s installation process or, as was more common, simply selected at random from an included list of stolen—yet valid—product keys. While the requirement of a valid Product Key was potentially enough to deter more honest—or less technically savvy—users from sharing copies of Windows, as a technology the early versions of Product Activation were hardly effective at providing a bulletproof solution to casual copying.

As broadband Internet installations among American consumers increased in the early 2000s, it became possible to add an additional layer to previous software activation processes: the online verification of individual CD or product keys via a central activation server. This approach had numerous advantages, not the least of which was the ability to ensure that a product key was only used once, in a single installation. For Windows XP, Microsoft implemented a new technical layer to the previous product key-based approach. A valid Product Key was still required at the time of installation and was verified by the installation process as

in the Windows 9x series. However, after successful installation, the user was then required to "activate" their copy of Windows by verifying the legitimacy of their operating system with Microsoft, either via the Internet (the preferred method) or by contacting a customer representative by phone.[14]

As described on Microsoft's TechNet website, the activation process was composed of several steps. The first of which is the creation of a hardware hash,[15] or a numeric value "created by running 10 different pieces of information from the PC's hardware components through a one-way mathematical transformation."[16] In other words, information about installed components inside the computer is used to produce a number somewhat unique to that computer. The hardware hash is then combined with the Product Key through another transformation to form the Installation ID, a 50-digit number which is then transmitted to Microsoft servers. Assuming the copy of Windows XP is valid and is not installed on another computer, Microsoft's activation servers then send back a digital certificate containing the activation key. The copy of Windows is then considered activated and valid. Users who did not have Internet access or were unable to successfully activate online had to call Microsoft's customer service and provide the Installation ID. If the Installation ID was valid, the customer service

14. Microsoft Corporation, "Microsoft Piracy - Piracy Basics."

15. Microsoft's online resources are incredibly inconsistent in their use of phrases both as common and proper nouns to refer to the same technologies across different publications and versions of software. "Product Key" is used interchangeably with "product ID," and the generic "hardware hash" becomes "Hardware ID" in other contexts.

16. Microsoft Corporation, "Technical Details on Microsoft Product Activation for Windows XP," *Microsoft TechNet*, last modified August 13, 2001, accessed October 22, 2016, https://technet.microsoft.com/en-us/library/bb457054.aspx.

representative would provide the user with a 42-digit Confirmation ID that the user then entered into the activation program.[17]

In addition to the initial activation of the operating system at the time of installation, Windows XP also re-checks the activation status on each boot. As the hardware hash is derived from installed components, if an advanced user were to upgrade or replace an installed piece of hardware, the hash would necessarily be different from the one computed at the time of installation and would signal to the operating system that the computer may not have been the same it was originally installed on. This was designed to prevent the practice of hard disk cloning, where an installed, activated system is directly duplicated onto another hard drive, preserving the activation status and allowing multiple users to work with the same copy of the OS. In an interview from May of 2001, Microsoft Product Manager of Activation Allen Nieman acknowledged that users have legitimate reasons to change the components inside their computers and said that Product Activation was designed to take this into account, tolerating a substantial amount of hardware changes before asking the user to re-activate the operating system. Nieman stated that “our goal is to make activation as flexible as possible” and that the Product Activation process could possibly overlook activity that would otherwise, to Microsoft, signify potential unauthorized duplication of the operating system. He noted that “we designed it to err on the side of the user. In other words, to allow activity that most people would agree is infringing so as not

17. Ibid.

inconvenience [sic] the honest consumer."[18] While ostensibly a benevolent dispensation for hobbyists who enjoy modifying their systems, this offhand statement illustrates a startling reality of Windows under the new Product Activation regime: a third party—*not* the user—would be the one to determine what is an allowable number of hardware changes a user could make to their machine, and deny user access to that machine if the allowable limit had been exceeded.

Even though Windows XP could be completely installed without completing the activation process, the operating system would still force the user to activate within a set time. Users have a grace period of 30 days from installation in which Windows must be activated; after that time, the user will not be able to access any programs or Windows features beyond the Product Activation application until the OS is activated.[19] Released later in Windows XP's lifespan, Microsoft's Genuine Advantage software acted as another layer of checking the validity of the operating system, displaying a persistent notification on the desktop that the copy of Windows may not be genuine and preventing users from downloading system updates beyond those that addressed critical vulnerabilities in Windows XP and later systems.[20]

18. Nate Mook, "The Truth About Windows Activation," *BetaNews*, last modified May 18, 2001, accessed May 7, 2017, https://betanews.com/2001/05/18/the-truth-about-windows-activation/.

19. Microsoft Corporation, "What Is Windows Product Activation?," *Microsoft - Windows Product Activation Overview*, last modified 2017, accessed November 3, 2016, https://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/wpa_overview.mspx?mfr=true.

20. Microsoft Corporation, "About Genuine Windows - Windows Help," *About Genuine Windows*, last modified June 14, 2017, accessed July 3, 2017, https://support.microsoft.com/en-

### User Reactions to Product Activation

Online reactions by users to the Windows Product Activation technology in the months leading up to the launch of Windows XP were understandably skeptical with regard to the activation requirement. At the same time, most discussion of the issue was tempered by a fatalistic tone of resignation along with a strangely optimistic wait-and-see attitude. As early as February 2001, when Microsoft announced the Product Activation technology in a press release,[21] online sources voiced their concern and speculated about the negative effects of this new initiative. Reporting on details available through unofficial sources shortly after the announcement, Ken Fisher of technology news blog *Ars Technica* stated that "for most enthusiasts, the Hardware ID makes us nervous. How many times can I upgrade my box before having to re-register or buy another copy of Windows?"[22] IT news site *The Register* provided a look into the closed beta-testing of Windows XP in March of that year, referring to newsgroup transcripts that "indicate continuing hostility (as you might expect from techies), and even seem to signal that the Microsoft *staff* minding the newsgroups aren't altogether enamored of the system either."[23] An anonymous tester stated that "my recommendation to my

---

us/help/15087/windows-genuine.

21. Microsoft Corporation, "Microsoft Anti-Piracy Solutions Extended to Upcoming Versions of Office, Windows and Visio Products Worldwide," *News Center*, February 2, 2001, accessed July 3, 2017, https://news.microsoft.com/2001/02/02/microsoft-anti-piracy-solutions-extended-to-upcoming-versions-of-office-windows-and-visio-products-worldwide/.

22. Ken Fisher, "Windows Product Activation: An Early Look," *Ars Technica*, last modified February 2, 2001, accessed November 3, 2016, http://arstechnica.com/information-technology/2001/02/wpa/.

23. John Lettice, "WinXP Beta Testers Still in Open Revolt over Product Activation," *The Register*, last modified March 20, 2001, accessed November 3, 2016,

customer will be to...stay away from Whistler [the pre-release code name for Windows XP], even if it's a very good OS, the activation process is too much trouble for whatever good the OS will give you in return."[24] It is unclear in this article whether the testers had actually experienced the Product Activation process, however, as other complaints by early testers seemed centered around issues that are nonexistent in the final release, such as the assumption that the replacement of single hardware components would necessitate a total reinstallation or reactivation.

An article from *PC World* later the same month asserted that "Microsoft's stepped-up copy protection may prompt even more howls from users," and speculated that "if you alter enough of the system's characteristics...by upgrading video, storage, and other components, for example—you may have to call Microsoft and convince a representative that you're not a software pirate before you can use the system again."[25] By May 2001, further details of the Product Activation system had been made publicly available, and the interview with Nieman attempted, among other things, to allay some of the fears of hobbyists that they will be unnecessarily restricted from replacing or upgrading hardware past a certain number of times. At this point in development, however, Nieman

---

http://www.theregister.co.uk/2001/03/20/winxp_beta_testers_still/.

24. Ibid.

25. Scott Spanbauer, "Latest Windows XP Beta Adds Strict Copy Protection," *PC World.Com* (March 25, 2001), accessed November 16, 2016, http://search.proquest.com/docview/200751519/abstract/C2FC31DD6A944DCFPQ/1.

was unable to confirm or deny any specific limitations, citing that some details had not fully been set.[26]

With Windows XP's release in late October 2001, more mainstream publications weighed in on the issue of product activation, though from a slightly different standpoint. Technology columnist Dave Wilson of the *LA Times* issued a scathing critique that "this feature is supposed to take aim at software piracy, but the truth is it's just another example of a rapacious monopolist abusing computer users who are helpless to do anything about it."[27] But Wilson didn't take exception to the fact that every installation of Windows XP must be validated by Microsoft from a privacy standpoint—instead, the larger issue was that "in the future, you'll have to pay for every copy of the operating system loaded on every computer you own," with Wilson lamenting the bygone days when Microsoft "turned a blind eye" to those practices.[28] Writing for the *New York Times*, J.D. Biersdorfer similarly said that "some computer enthusiasts expressed dismay that they would now have to buy a copy of the system for each PC that they chose to upgrade," while also conceding that the end-user license agreement—"the long legal statement that most users affirm with a click without reading while installing new software"—had always limited the installation of previous versions of Windows to just one PC.[29] While Biersdorfer did acknowledge privacy concerns voiced by some potential users about what sort of information is shared with Microsoft and how

26. Mook, "The Truth About Windows Activation."

27. Dave Wilson, "Safeguards Punish Consumers, Not Pirates," *Los Angeles Times*, October 25, 2001, accessed November 3, 2016, http://articles.latimes.com/2001/oct/25/news/tt-61351.

28. Ibid.

much influence the software will exert over the user's system remotely, the two newspaper writers shared in their outrage at a technological solution enforcing licensing terms—and ironically seemed to situate themselves as the type of users Microsoft designed this system to combat in the first place.

David Coursey of ZDNet also stated his unhappiness with the newfound license enforcement, though with a bit more grace than his colleagues at the newspapers: "sure, making copies of Windows 98 was illegal, but there really wasn't any way to stop you. And if you copied the software onto a second home machine, say, it really did not seem wrong. But with XP it is wrong, and you cannot plead ignorance."[30] Discussing privacy concerns later in the article, Coursey said that he took Microsoft's stated concern with user privacy at face value and was more concerned with the possibility that information communicated to Microsoft's servers as part of the activation process could possibly be accessed or intercepted by malicious third parties—a relatively unique concern in the discussion surrounding Product Activation.

Perhaps the most telling reaction—to be examined further in the following section—was published by *Maximum PC* magazine, a publication geared towards enthusiasts with a focus on testing and reviewing PC hardware that generally took an irreverent, anti-authoritarian tone in its writing. In a Windows XP preview in

29. J. D. Biersdorfer, "PIRACY AND PRIVACY; Dear User: This Bootleg Copy Will Self-Destruct in 30 Days," *The New York Times*, September 6, 2001, accessed November 16, 2016, http://www.nytimes.com/2001/09/06/technology/piracy-and-privacy-dear-user-this-bootleg-copy-will-self-destruct-in-30-days.html.

30. David Coursey, "Top 10 Things You MUST Know about Win XP," *ZDNet*, last modified October 25, 2001, accessed June 30, 2017, http://www.zdnet.com/article/top-10-things-you-must-know-about-win-xp/.

the October 2001 issue, Will Smith described the magazine's uncharacteristically temperate position: "at *Maximum PC*, we have two concerns about Product Activation: that it will prove to be a pain for people who frequently upgrade their hardware, and that it will allow Microsoft to form a database of users' hardware configurations."[31] Outside of Microsoft's own TechNet publication, this article provides the most technologically comprehensive explanation of the Product Activation process, and does support Microsoft's own claims that the process does not produce any personally-verifiable information that could be used to identify individual users. Smith concluded by saying that the magazine's staff fully supports the right of software developers to protect their products from illegal duplication, but not to the extent that it invades the user's privacy or makes everyday use difficult, threatening that "if Product Activation forces us to call Microsoft tech support every time we want to install a new videocard or CD burner in a test bed, we'll be a very unhappy bunch of campers."[32]

**The Banality of Verification**

Windows XP was the first major operating system to require users to verify their copy of the software with its creator via the Internet, and as described previously this represented a substantial change even for those who were used to the anti-counterfeiting measures attempted through the use of offline CD or product keys. With the requirement of what was essentially securing Microsoft's

31. Will Smith, "The 10 Most Important Things You Must Know About Windows XP," *Maximum PC*, October 2001, 47.

32. Ibid.

approval and blessing in order to use the latest version of the Windows operating system, it would be reasonable to assume that users would be understandably concerned about potential privacy implications of this requirement. Yet while many contemporary writings did indicate some small amount of unease at the new arrangement, most of the discontent involved other potential consequences of Product Activation. Major newspapers from both coasts complained about the enforcement of the end-user license that prohibited the installation of a copy of Windows on more than one computer—a provision extending as far back as Microsoft's MS-DOS operating system which preceded Windows. Now in the case of XP, however, the terms of the license were enforced by the software which actively prevents violation of the license—a perfect real-world expression of Lawrence Lessig's dictum that "code is law."

Lessig further points out that—like it or not—verification is, in some contexts, an inescapable part of online life. As an example, Lessig cites two complete opposite policies of Internet access at the University of Chicago and Harvard University in the mid-1990s. The former treated Internet access as an extension of protected First Amendment speech, while the latter was concerned with preventing unauthorized use of the university network, and required all users to first pass through an authentication process to confirm whether they were students or faculty of the university.[33] Harvard's approach of authentication and control is now more the norm than the University of Chicago's, with relatively few

33. Lawrence Lessig, *Code: And Other Laws of Cyberspace, Version 2.0* (New York: Basic Books, 2006), 33–34.

holdouts in the modern age treating open access to the Internet as an issue of free speech (libraries are one of this notable minority, and are the subject of discussion in Chapter Six). Yet as Lessig goes on to explain, verification is a common, nearly invisible and potentially daily process in the "offline" world: a driver's license provides authentication to buy age-restricted products such as beer or cigarettes, and the practice of signing credit card receipts in stores is checked against the signature on the back of the credit card to presumably confirm that the individual making a purchase is the actual individual to whom the card had been issued.[34] These various, discrete tokens of identification also have the advantage of not revealing more information than they have to: an accepted signature matched to a Visa card says nothing about the owner's date of birth or physical place of residence, for example, while a driver's license used to confirm a customer is old enough to buy alcohol gives no indication as to their current credit status.

One potential point of critique of the new order imposed by Product Activation under Windows XP is that it seems to extend past Lessig's model of individual tokens of authentication for separate purposes. The previous means of activation, using the CD key present on the Certificate of Authenticity to determine whether the installation process would be allowed to complete or not, relied on a token of verification specific to—and entirely useless outside of—the context of software installation. But Microsoft's concern over illegal copying led to the XP model of Product Activation, which now demands, in addition to the Product Key, specific information about the user's hardware as part of the overall

34. Ibid., 50–51.

activation process. The previous practice of requiring just enough information to authenticate has been supplanted by a requirement for extraneous information which, in the case of Windows XP's product activation, has been made an integral and inseparable part of the activation process, but which, in the more theoretical terms of a minimum amount of information needed to verify the user is installing a legitimate copy of the software, is not strictly necessary. The user is already (presumably) in possession of a legitimate product key; in extending Lessig's example, the Product Activation process would be akin to a secondary age check implemented when the customer attempts to consume their legally-purchased beer in their home.

But theoretical discussion of whether an authentication mechanism exceeds a reasonable requirement of information is irrelevant in light of how these practices are perceived by the user. The reaction of *Maximum PC* magazine seemed to perfectly exemplify the broader attitude about this new restriction: if Product Activation works and is minimally intrusive, then there is no problem. If it becomes an impediment to upgrading and repairing components—at that time and still today largely the domain of hobbyists rather than the average user—then there will be a problem. The requirement of activation was otherwise not viewed as any sort of terrible incursion on the sovereignty of the user, and any privacy concerns were not enough to keep Windows XP from overwhelming success and a lifespan of over a decade. Potential privacy issues in Product Activation just did not seem to dissuade potential users. Part of this may have been a result of the

great pains Microsoft took to continually reassure potential users that the data transmitted during the activation process could not be used to identify individual users or their hardware. And in all fairness and with the benefit of several years since the operating system was discontinued, there has been no evidence to suggest that the activation process was less secure or anonymous than Microsoft claimed. The long tail of Windows XP's legacy arguably lives on in a number of ways: the online verification of software is commonplace today with the ubiquity of always-on broadband Internet connections, and many software developers are taking these practices of user verification even further by taking a software-as-a-service (SAAS) approach and hosting their software entirely in the cloud.[35]

But how does this minimally-intrusive activation process that affects the user of an operating system relate to the broader figure of the Internet user? The two groups would seem to have no conceptual connection beyond the obvious: that an Internet user may very well surf the web from a computer running Windows XP. But there are two parallel threads that converge into something larger that certainly does concern the Internet user: the imposition of a verification process—easily extrapolated to less-anonymous processes of identification as will be shown in the following chapters—as a precondition to the use of software, and ultimate indifference to these processes of verification so long as they are suitably hidden from the user and don't intrude into the everyday experience.

35. For examples, see Adobe's Creative Cloud, an online replacement to its Creative Suite set of graphical tools or Microsoft's own Office365, which replaces the discrete ownership of its Office software suite with a yearly subscription-based model.

Windows XP was a critical step in the normalization of processes of verification for the user. For the first time, the operating system—the most fundamental piece of software on a computer—must report back to its creator before it is allowed to run as intended. No longer was the user entirely free to do with as they pleased after they purchased this essential piece of software; the user must now always gain permission from the software's creator—who may be checking in from time to time. Discussion of the Product Activation technology operates in terms of verifying the legitimacy of the software being activated, but the real object of this scrutiny is the user. Is the user legitimate—that is, did they obtain the copy of the software they are attempting to run through sanctioned channels? Are they attempting to run a counterfeit version of the software, or install it on more than one computer? In essence, Product Activation is policing the actions of the user, not the software, in order to enforce compliance with licensing terms the user was never able to negotiate.

This legacy also has implications for discussions of software "ownership." As software developers increasingly attempt to argue that software is not so much "owned" by the user/consumer as it is "licensed," thus placing the user in a continual state of dispossession: no longer the legitimate owner of a software program but its tenant, using it according to the pleasure of the developer. In this reframing, the only legal power generally allowed the user should they not agree to the terms of the license is to discontinue the use of the software entirely, but when the software at stake is the very thing that allows a computer to be anything

more than an over-sized doorstop, how much choice does the user truly have in this arrangement? And more importantly, when the user only sees this restriction of their autonomy as little more than a possible inconvenience at certain infrequent occasions, these tools of control become seen as necessary evil—if even in such strong terms, and more likely are viewed as the cost of participation in the modern, connected world. Successive requirements of verification and other technologies of control are met with less and less resistance as these processes become normalized.

## Conclusion

It's reasonable to assume that the obvious concern about Product Activation and similar technologies would be with regard to user privacy, but as the user responses above suggest, privacy concerns are minimal at best in comparison to questions regarding hardware upgrades. And in some ways, to focus on the issue of privacy in the transmitted activation data is to miss the point about the larger concern: the precedent set by this development, and the relative indifference on the part of the users. The inclusion of the Product Activation technology in Windows XP is, if not objectively the first, then one of the most visible starting points for the gradual disempowerment of the user: the requirement of verification. The legacy of this is that the user is now continually verified in their use of services on the Internet as well as nominally "offline" software—and moreover, the user *expects* to be verified, anticipates it and is entirely complacent towards the whole process. The loss of this degree of freedom

is accepted without complaint, as long as the verification process remains in the background and doesn't interrupt everyday use.

In Chapter VI, I will revisit the verification of the user in a related context, 14 years later, to examine one discursive and legal consequence of this particular precedent. Whereas with Windows XP, the user is verified in order to ensure their legitimate ownership of the software—we could say verified in order to ensure their legitimacy *as a user*—the case study presented in Chapter VI shows verification as now a mandatory part of online participation, with substantial consequences for failing to be verified. The total visibility of the user online has become the norm, and attempts to evade or otherwise confound processes of verification now are discursively attached to the suggestion of deviance or criminality.

The next chapter serves as a bridge between these two ideas in examining the role of advertising as it has emerged as the dominant structural logic of the Internet. Targeted advertising requires the collection of ever-more detailed data on the user's habits for the production of increasingly sophisticated advertising profiles. Without some form of verification, of aggregating otherwise discrete data points into a model representing a physical user, targeted advertising loses its effectiveness. As we will see in the following case study, the verified user is vital to these advertising practices, and substantial effort is placed into producing discourses that reinforce the user's responsibilities and expected behavior—and corresponding loss of agency—within the hegemony of online advertising.

# CHAPTER V

# CASE STUDY II: THE USER IS TRACKED—ONLINE ADVERTISING AND ADBLOCK PLUS

## Introduction

Capitalism has always been the barbarian at the gates of the Internet. The desire of telecommunications companies to tap into an entirely new market through the sale of Internet access was one of the primary motivating factors for the privatization of the network infrastructure in 1995.[1] And it wasn't long after the birth of the Internet that advertising companies began to realize that the Internet could revolutionize the way advertising was done. The Internet promised a drastic change from previously one-way technologies of mass communication such as television and radio, and that interactivity also promised new ways for advertisers to reach potential consumers. Attempts by advertisers to take advantage of the possibilities of online communications actually began several decades before the formal birth of the Internet: what is widely regarded as the first spam email was sent over the ARPANET in 1978 (and about 15 years before the term "spam" was used to describe such mailings). A marketing representative of the Digital Equipment Corporation sent an email to hundreds of ARPANET users to announce an upcoming computer model that DEC was developing. Due to both an error that caused the addresses of many recipients to be printed in the body of the message as well as the self-promoting nature of the announcement (not to mention that it was written in all capital letters, a hallmark of spam to this

1. Janet Abbate, *Inventing the Internet* (Cambridge, MA: MIT Press, 2000), 196–197.

day), the first spam was understandably met with general hostility from the affected users.[2]

This initial attempt could hardly be considered a success, yet it contains all the hallmarks of online advertising decades later: unsolicited announcements of products or services, an obnoxious visual presentation, and the rationale that the product was something useful to the recipients. And while this ur-spam certainly illustrated the ease with which advertising could impose upon large numbers of users with little effort, there was nothing in this incident that came close to anticipating the overwhelmingly intrusive possibilities of online advertising that would follow decades later. The critical difference between traditional, or offline, advertising and online advertising lies in the two-way nature of online communications, or as David Evans describes in his overview of the online advertising industry, "the fact that advertisers (and their intermediaries) know with confidence what content a particular consumer is viewing, [which] allows advertising to be targeted."[3] This knowledge of the user's content consumption extends past the particular web page they may currently be viewing to the search keywords they used to arrive at the page as well as their recent search and browsing history. What is particularly concerning about this is the way that these processes of user tracking are nearly entirely invisible to the common user, and are designed to exploit the use of popular web services to continually extract more

2. Brad Templeton, "Reaction to the DEC Spam of 1978," accessed July 8, 2017, http://www.templetons.com/brad/spamreact.html.

3. David S. Evans, "The Online Advertising Industry: Economics, Evolution, and Privacy," *The Journal of Economic Perspectives* 23, no. 3 (2009): 42.

data in order to produce an ever-more refined advertising profile of the user. Chris Hoofnagle et al. state that "behavioral advertising—and the tracking that goes with it—is the offer that you cannot refuse, not necessarily because you are tempted by it, but because sophisticated, market-dominant actors control the very platforms you use to access the web."[4]

This chapter is concerned with the phenomenon of adblocking software, which enables users to block advertisements and associated attempts at behavioral tracking online. The advertising industry has continually opposed attempts at implementing government regulation of advertising practices, and manages to weaken the few regulatory victories which benefit the user.[5] Technologically-savvy users have responded by developing adblock software in order to provide users with the autonomy that is denied them both by the advertising industry and by the government, in its failure to regulate on behalf of the user. This software has of course generated controversy, given the ubiquity of online advertising as the source of primary revenue for the majority of websites. To the users, adblocking software is an opportunity to restore lost agency and resist the current structures of the Internet which have normalized and made inescapable the practices of tracking and advertising. For advertisers, adblocking is an attack on the self-proclaimed mandate to profit from the online ecosystem in whatever means possible, an unfair violation of an implied social contract and a

4. Chris Jay Hoofnagle et al., "Behavioral Advertising: The Offer You Cannot Refuse," *Harvard Law & Policy Review* 6, no. 2 (2012): 278.

5. Ibid., 275–276.

genuine threat to revenue. And there is a third party with a stake in the development of this technology as well: that of website owners who have come to rely on advertising to meet their operating expenses,  While not necessarily ideologically opposed to user autonomy and privacy, website owners nonetheless are aligned with the advertising industry in their acceptance of its business model and ideological rhetoric.

This chapter will focus specifically on one event that brought practices of adblocking, previously confined to the more technically-minded Internet users, into a broader public conversation: the decision of the creator of Adblock Plus, once the most popular adblocking program, to create an "Acceptable Ads" program that allowed advertising companies to have their advertisements "whitelisted," or allowed through Adblock Plus and displayed to the user as long as the ads met certain aesthetic criteria.[6] Advertisers were required to pay a small percentage of their advertising revenue to be included in the Acceptable Ads program. This decision was distasteful to both the users, who considered it a betrayal of the implied purpose of adblocking software as well as to the advertising industry, which considered the move a brazen shakedown attempt by software that was already seen as affecting revenue. This particular event will serve as a focal point for examining and critiquing the ideological narratives of online advertising practices, the normalization of rhetoric that posits advertising as both a sustainable economic model as well as a revenue stream that website

6. Wladimir Palant, "Allowing Acceptable Ads in Adblock Plus," *Adblock Plus and (a Little) More*, December 5, 2011, accessed July 6, 2017, https://adblockplus.org/development-builds/allowing-acceptable-ads-in-adblock-plus.

owners and advertising companies are entitled to, and the subsuming of the user's privacy and autonomy under capitalist practices of commodification and exploitation.

## A Brief History of Advertising Online

Advertising on the Internet began with the humble banner ad, an initially static image of 468 by 60 pixels that sat at the top of a webpage and displayed content from the advertising organization. The first banner ads appeared on HotWired, the online version of technology culture magazine *Wired*, with 14 individual companies including AT&T and Volvo (as well as now-defunct contemporary examples like MCI, Zima, and 1-800-Collect) participating. The banner ad tracked the number of users who had visited the page (and presumably viewed the ads), as well as the number that actually clicked on the banners.[7] As many companies were still building their web presence at the time, just what the banners linked to when clicked was something of a mystery—AT&T's ad led not to the company's webpage but to a landing page that connected with it contemporary "You Will" television campaign, which detailed the (somewhat prescient) changes to modern life that the Internet would bring.[8] The landing page detailed the possibilities of touring virtual art museums online and provided links to information on present and coming Internet technologies.[9] The implication, of course, was that the Internet service would be provided over the

7. Ryan Singel, "Oct. 27, 1994: Web Gives Birth to Banner Ads," *WIRED*, October 27, 2010, accessed July 8, 2017, https://www.wired.com/2010/10/1027hotwired-banner-ads/.

8. Rebecca Greenfield, "The Trailblazing, Candy-Colored History Of The Online Banner Ad," *Fast Company*, October 27, 2014, accessed July 6, 2017, https://www.fastcompany.com/3037484/the-trailblazing-candy-colored-history-of-the-online-banner-ad.

AT&T telephone service the user was subscribing to, but overall the advertisement was surprisingly informational. Craig Kanarick, a freelancer who worked for the advertising company that produced the campaign, recalls thinking, "let's not sell somebody something. Let's reward them for clicking on this thing brought to you by AT&T."[10] It goes without saying that this approach would be considered bizarrely old-fashioned and entirely ineffective in today's advertising landscape. But for the time—possibly as an effect of the novelty for a population still acclimating to the online world—HotWired's banner ads were a resounding success, boasting a click-through rate (the number of viewers who actually click on the advertisement) of 44%, while today a banner ad is more likely to have a click-through rate of 0.08%.

From the relatively innocuous banner ads came the pop-up advertisement. Pop-up ads were created by the webpage hosting company Tripod.com, which scanned the homepages created by the company's users in order to show banner ads that were more closely targeted to the user's presumed interests. This same approach is used, for example, by Google in generating related advertisements on its Gmail service through the automated processing of a user's email messages,[11] but Tripod encountered a particular problem. As described by Ethan Zuckerman, a former Tripod employee and the creator of the pop-up ad, "specifically, we came

9. While the original AT&T website for this campaign is long gone, see http://www.thefirstbannerad.com/ for an archived version of how the ad would have appeared in 1994 as well as additional context and information.

10. Greenfield, "The Trailblazing, Candy-Colored History Of The Online Banner Ad."

11. "Privacy & Terms," *Google Terms of Service*, accessed July 11, 2017, https://www.google.com/intl/en/policies/terms/.

up with [the pop-up ad] when a major car company freaked out that they'd bought a banner ad on a page that celebrated anal sex."[12] The pop-up ad was a way of showing advertising content on a webpage, but without the implied association between the advertiser and the hosted webpage's content.

In 1996, the DoubleClick advertising agency was created and brought a new focus to online advertising campaigns. Previously, advertisers had to manually track any advertising campaigns they may have been running on multiple websites, and finding websites to purchase advertisements was left entirely to the advertisers. DoubleClick provided a convenient middleman for everyone concerned: by representing multiple advertisers, DoubleClick provided a one-stop solution for website owners looking to host ads on their sites, and for advertisers DoubleClick simplified the effort of finding customers as well as providing the unprecedented ability to track advertising campaigns across multiple websites, and users through their interactions with the various campaigns.[13] This was done through the use of a file called an HTTP cookie, which was originally designed to carry persistent information about the user's session across a number of related but largely static web pages; a somewhat quaint example in the original specification poses a hypothetical online store in which a "shopping cart" could store the item a user intends to purchase as they

12. Ethan Zuckerman, "The Internet's Original Sin," *The Atlantic*, August 14, 2014, accessed July 6, 2017, https://www.theatlantic.com/technology/archive/2014/08/advertising-is-the-internets-original-sin/376041/.

13. Ankit Oberoi, "The History of Online Advertising," *AdPushup Blog*, July 3, 2013, accessed July 10, 2017, https://www.adpushup.com/blog/the-history-of-online-advertising/.

browse through different pages representing the various items for sale.[14] For over a decade, the cookie would be one of the central technologies behind both online advertising and the software tools designed to block it.

Google debuted the AdWords program in 2000, which further refined the ability of advertisers to create targeted ads from user browsing habits. As a contrast to the increasingly garish visuals of banner and pop-up ads, AdWords placed short paragraphs advertising products or services related to the user's search keywords alongside the search results on Google's webpage. The initial AdWords press release stated that this targeted approach "enhances the overall search experience for Google users by providing relevant, useful information on the search results page, and benefits advertisers by increasing the likelihood that users will click on a specifically targeted ad."[15]

The dot-com bubble burst in 2000–2001, taking with it much of the growing excess of commercial "Web 1.0" culture. A few years later, the growing hype over Web 2.0 pushed for a drastic re-imagining of the Internet ecosystem, one which situated the user more firmly within the new economy. The banner ads of Web 1.0 mirrored real-world advertising in print and on billboards, where viewers—who and how many—were largely unknown to the advertisers. But under the logic of Web 2.0 that pushed increased interactivity between the user

14. David M. Kristol and Lou Montulli, "RFC2109 - HTTP State Management Mechanism" (Internet Engineering Task Force, February 1997), 2, accessed July 10, 2017, https://tools.ietf.org/html/rfc2109.

15. "Google Launches Self-Service Advertising Program," *News from Google*, last modified October 23, 2000, accessed July 10, 2017, https://web.archive.org/web/20120313164802/http://www.google.com/press/pressrel/pressrelease39.html.

and websites, these static and unquantifiable methods were entirely unacceptable. In the initial aftermath of the dotcom bust, advertisers relied heavily on pop-up ads, but with the growing presence of pop-up blocking software and strong user dislike of the format, the pop-up was soon abandoned in favor of more subtle, nuanced approaches.[16] AdWords emerged in the middle of the bust and seemed to provide the template for advertising of the future: a focus more on targeted, relevant ad placement instead of the previous mass communication-inspired approaches which relied on a wide placement of ads which may not have been relevant either to the users or in the context of the websites on which they appeared. The future of Internet advertising was in ads targeted at a specific user, and that meant discovering—and retaining—the user's interests.

### The User is Always Tracked

By its very nature, online advertising is incompatible with user privacy. The days of the static banner ad, running for a certain period of time on a specific place on a website, at a specific advertising rate, have long receded into the past. Technology now allows for advertising to be more closely targeted to the hypothetical interests of the user thanks to the ability to monitor, in real time, the user's online activities and add every scrap of information to an increasingly detailed profile. For example, a network analysis performed by Richard Gomer et al. found that in only 30 clicks on results from a search engine, the average user would find themselves tracked by the 10 most active online advertising entities.[17] HTTP cookies have long been the basis for most online tracking as they present an

16. Oberoi, "The History of Online Advertising."

easy way for websites to both record information about the user as well as see where the user has been. However, cookies are also one of the easiest tracking technologies to foil—the user simply has to delete them from their computer, and the advertiser loses all record of that user's aggregate activities.[18] And when tools like adblocking software are employed, advertisements on web pages are prevented from setting cookies in the first place. To avoid losing this valuable advertising data, advertisers have attempted to find solutions that are far more persistent and difficult for the user to evade. Verizon received a significant amount of negative press in 2015 when it was revealed that it was tracking its mobile subscribers across the Internet with a technology that regenerated tracking cookies—nicknamed "zombie cookies" or "evercookies"—that had previously been deleted by users.[19]

To the extent that users are made aware of how their online actions contribute to the profiles produced by advertising networks, the details are often obfuscated in tedious and confusing terms of service that are frequently clicked through so the user can begin using the services they've signed up for. When users

---

17. Richard Gomer et al., "Network Analysis of Third Party Tracking: User Exposure to Tracking Cookies Through Search," in *Proceedings of the 2013 IEEE/WIC/ACM International Joint Conferences on Web Intelligence and Intelligent Agent Technologies*, vol. 1 (presented at the 2013 IEEE/WIC/ACM International Conference on Web Intelligence, Atlanta, GA: IEEE Computer Society, 2013), 556, accessed July 6, 2017, http://dx.doi.org/10.1109/WI-IAT.2013.77.

18. Robert W. Gehl, "The Online 'Cookie' Has Turned Stale. Here's What Advertisers Are Cooking up to Replace It.," *The Week*, February 18, 2014, accessed July 6, 2017, http://theweek.com/articles/451231/online-cookie-turned-stale-heres-what-advertisers-are-cooking-replace.

19. Julia Angwin and Mike Tigas, "How This Company Is Using Zombie Cookies to Track Verizon Customers," *ProPublica*, last modified January 14, 2015, accessed July 15, 2017, https://www.propublica.org/article/zombie-cookie-the-tracking-cookie-that-you-cant-kill.

are given a clear explanation as to what data is used and how, the explanations of the processes by which this data is monetized and what third parties it is sold to are entirely opaque. Most importantly, there is no single point from which to opt out of advertising: while parts of the advertising industry nominally provide a one-stop solution for users to opt out of tracking by advertising networks,[20] the reality is that the user is negotiating their opt-out status with over 100 different companies. As Robert Gehl and Casey Boyle noted, "you will see that you're entering into a contract not with the *advertising industry as a whole* but rather (at the time of this writing) 117 ad networks. There is no negotiation with such a swarming entity."[21] Of course, deleting any of the cookies set on the user's machine that indicate their opt-out status then produces the assumption that the user is not opposed to being tracked on their next visit to one of the participating sites. The user will also have to perform this opt-out ritual on every device they use to access the Internet since the opt-out cookies are limited to a local machine. In addition, the processes of completely opting out of targeted advertising are not —nor are they designed to be—accessible and transparent to the average user. Pedro Leon et al. examined the processes and tools for opting-out of or otherwise blocking online advertisements, and found that "the status quo is insufficient for

20. Digital Advertising Alliance, "WebChoices: Digital Advertising Alliance's Consumer Choice Tool for Web (Beta)," accessed July 11, 2017, http://optout.aboutads.info/.

21. Robert W. Gehl and Casey Boyle, "Cookie Cutters," *The New Inquiry*, March 20, 2014, accessed July 6, 2017, https://thenewinquiry.com/cookie-cutters/.

empowering users to protect their privacy"—noting that "the status quo" means the self-regulatory approach taken by the online advertising industry.[22]

The "Do Not Track" standard proposed by the World Wide Web Consortium, the group that develops standards for the World Wide Web, attempts to provide a simple option in most web browsers that allows the user to indicate their wish not to be tracked by the websites they visit. However, the setting is almost entirely ornamental, as the user protections afforded by that setting are entirely voluntary on the part of advertisers. For example, Microsoft enables the "Do Not Track" setting on installations of its Edge browser in Windows 10 by default. In explaining why it will not honor this setting broadcast by the Edge browser, Yahoo stated that the default "on" setting did not represent "explicit user consent" with Do Not Track policy, and so would be considered invalid.[23] The irony of this position should be noted, given the advertising industry's general preference for assuming the user's consent to advertising and forcing the user to opt-out of advertising rather than letting them opt-in in the first place. There is what appeals to be a willful ignorance—or extremely literal interpretation—of what it means for the user to signify their rejection of online behavioral tracking; all else is an implied "yes." In the case of the zombie cookies used by Verizon, the company which developed the technology "does not consider [it] a signal that

22. Pedro Leon et al., "Why Johnny Can't Opt out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '12 (New York, NY, USA: ACM, 2012), 598, accessed July 6, 2017, http://dx.doi.org/10.1145/2207676.2207759.

23. Scott Gilbertson, "Yahoo, Microsoft Tiff Highlights the Epic Failure of 'Do Not Track,'" *WIRED*, October 29, 2012, accessed July 15, 2017, https://www.wired.com/2012/10/yahoo-microsoft-tiff-highlights-the-epic-failure-of-do-not-track/.

users want to opt out from being tracked" when they delete cookies from their phone or computer.[24] Do Not Track is essentially defanged by the lack of consensus among advertising entities on what constitutes "tracking" in the first place, and what actions advertisers should take when a user has enabled the Do Not Track setting.[25] The lack of explicit direction means advertisers are free to interpret Do Not Track as they see fit—and as often happens in the event of self-regulation, the industry and its component companies will honor the interpretation that benefits it the most.

The difficulty a user faces in opting out or otherwise blocking the tracking that accompanies online advertising illustrates a number of ideological structures that at this point are nearly inseparable from the shape of the Internet itself. Zuckerman notes that from the earliest days, "advertising became the default business model on the web, 'the entire economic foundation of our industry', because it was the easiest model for a web startup to implement, and the easiest to market to investors."[26] But it is possibly more correct to say that advertising is largely the animating logic of the Internet. The advertising industry's reliance on user data—and the absolute hegemonic control of the industry over the Internet—means that there is literally no value to the user who has opted out of tracking, or takes measures to block themselves from the all-seeing eye of the advertising industry; thus, there is no incentive for the industry to either make this process

24. Angwin and Tigas, "How This Company Is Using Zombie Cookies to Track Verizon Customers."

25Leon et al., "Why Johnny Can't Opt out."

26. Zuckerman, "The Internet's Original Sin."

simple or effective. Gehl notes the immediate inversion of expectations: "instead of agreeing to an opted-out status, we find that we have always *opted in*—even when we accept their consent to not track our online activities. We are, it seems, already opted out of opting out of such efforts."[27] In other words, we are always already opted in. Hoofnagle illustrates the irony in the disproportionate distribution of power online, noting that while the advertising industry objects to overly-strict (and pro-consumer) privacy regulations as being "paternalistic" and by extension against the principles of a free market, "advertisers are so invested in the idea of a personalized web that they do not think consumers are competent to decide to reject it."[28]

### Adblocking and the Empowered User

The development of technologies to block advertisements has allowed the user to take more control over their browsing experiences. Early advertisements featured garish colors, blinking text, or the especially reviled pop-ups/pop-unders, all of which were intrusive and disrupted users' browsing experiences. The limited expansion of broadband Internet in the early days of the web meant many users were browsing on dial-up connections over the phone lines, meaning that ad-heavy websites could substantially slow down the loading times. Always-on broadband is a much more common feature in the average American home, but the data cost of loading advertisements is still a concern for users on mobile devices, which often have strict data caps. And the advertising of today is more

27. Gehl and Boyle, "Cookie Cutters."

28. Hoofnagle et al., "Behavioral Advertising," 273.

than just a visual annoyance or one that slows down the speed of web browsing: the tracking of users performed in the service of increasingly relevant targeted advertising presents substantial concerns from a perspective of user privacy.

As with the telemarketing industry before it, the online advertising industry has been heavily resistant to government regulation of its marketing or even privacy practices, opting to either self-regulate in an attempt to preempt heavy-handed government involvement, or actively work to undermine and reduce the privacy protections for legislation that is enacted.[29] Lacking regulatory support, users concerned with the effects of advertising have been forced to resort to technological measures to resist the effects of online ads. Pop-up advertisements were the first advertising technology to come under sustained opposition: the Mozilla Foundation included a pop-up blocker in its Mozilla browser suite[30] as early as 2000, and in a slightly-delayed response, Microsoft itself provided pop-up blocking functionality in an update to the Internet Explorer 6 browser in 2004, as part of the Windows XP Service Pack 2.[31] Today, to the extent that it is needed, pop-up blocking is a basic feature in every major web browser. However, previously noted, the use of pop-up advertisements greatly decreased in the mid-2000s as targeted behavioral advertising became more effective.

---

29. Ibid., 274–276.

30. The Mozilla Suite included a browser, email client, and several other tools as a spiritual successor to Netscape's Communicator software. The browser portion of the code would eventually provide the basis for what would become the Firefox browser.

31. "Windows XP Service Pack 2: What's New for Internet Explorer and Outlook Express," *Microsoft.Com*, last modified August 4, 2004, accessed July 6, 2017, https://web.archive.org/web/20051212084214/http://www.microsoft.com:80/windowsxp/sp2/ieoeoverview.mspx.

As advertising technologies grew more pervasive, technology to defend users from advertising evolved to keep pace. Extensions, small programs that extend the functionality of a web browser, were released to block webpage advertisements first in Firefox and then in other browsers as the ability to run user-created advertisements was added to Chrome, Safari, and Internet Explorer. Adblocking extensions work by using filter lists of known advertising websites and then blocking the files from those locations when a webpage attempts to load them. This not only helps save bandwidth in preventing advertising data from being sent to the user's computer, but has the potential to reduce the load on the computer for ads that feature sound and video. A secondary function of most adblocking programs is more cosmetic: webpages which might otherwise be cluttered with advertisements become visually cleaner when ads are unable to load. Filter lists to popular adblock extensions are provided by the extension's developer, but other users can generally submit their lists as well, allowing any user a broad range of potential advertising and tracking sources to block. Adblocking software also provides the capability to "whitelist" advertising either from certain providers or on certain pages; the justification is that users can "show support" to websites they like or visit frequently by allowing ads to be shown on those pages. Given that adblocking software is generally intended to allow the user to have greater control over their web experience, the general convention is that the user is given the agency to decide which advertisements to allow, and by default most adblocking extensions come with no advertising sites whitelisted.

## The Battle over Adblocking

While there are a substantial number of extensions that provide some amount of adblocking functionality, arguably the most well-known adblocker is Adblock Plus, an extension for most popular web browsers such as Firefox and Chrome. In addition to being the most-used adblocker, Adblock Plus is well known for in the debate over the ethics of blocking online ads, and for the later controversy over the decision of the developer to allow certain advertisements by default. Adblock Plus began as Adblock in 2002 but was abandoned by its developer a year later. As the program was open source, an interested user, Michael McDonald, created a fork of the program in 2005 which improved on a number of features and was renamed Adblock Plus. Wladimir Palant took over development of the extension in 2006 and has been the lead developer since.[32]

In 2007, an otherwise unknown web developer named Danny Carlton (writing, inexplicably, as "Jack Carlton") posted a diatribe on his personal blog that argued that adblocking was tantamount to theft.[33] He stated that "FireFox [sic] allows and endorses the use of ad blockers," and as there was no reliable way for website owners to detect and block adblocking extensions, he would just block access to his website for all users with the Firefox browser (Carlton apparently did not understand that extensions are developed by individual third parties, not by Mozilla itself). Despite running a website that didn't seem to get

32. "About Adblock Plus," last modified November 19, 2010, accessed August 9, 2017, https://web.archive.org/web/20101119073306/https://adblockplus.org/en/about.

33. Danny Carlton, "FireFox Is Now Blocked from This and Many of My Other Sites," *JackLewis.Net*, August 4, 2007, accessed July 11, 2017, http://jacklewis.net/weblog/archives/2007/08/firefox_is_now.php.

much traffic to begin with—much less stand to lose out on advertising revenue through the use of adblocking extensions—Carlton's crusade against Firefox was reported on by a number[34] of online news sites[35] at the time.[36] While Carlton's battle shortly faded out of the public consciousness, this small incident represented the first visible discussion about the use of adblocking software.

Carlton's post marked the beginning of a genre of opinion pieces and blog posts wherein concerned website owners would discuss the negative effects that adblocking was having on their business, and implore the readers to either disable adblocking software entirely, or at least make an exception for that particular site by adding it to the user's whitelist. These articles are generally posted in small-to-medium-sized websites; larger news sites have either instituted paywall systems allowing users a certain number of free articles per month before they are required to subscribe (such as the *New York Times*) while others like *The Guardian* have taken to including a small banner image at the top or bottom of webpages that asks readers to either disable adblocking or support the site through a voluntary donation. As an example of this genre, two widely-read websites, technology enthusiast blog *Ars Technica* and video game reporting site *Destructoid* both penned lengthy articles trying to convince their users to stop blocking ads.

34. Paul McDougall, "Firefox AdBlock Foe Calls For Mozilla Boycott," *InformationWeek*, last modified September 12, 2007, accessed July 6, 2017, http://www.informationweek.com/firefox-adblock-foe-calls-for-mozilla-bo/201805865.

35. Jack Schofield, "Ad Blocking Is Theft, so Block Firefox Instead (Updated)," *The Guardian*, August 19, 2007, sec. Technology, accessed July 6, 2017, https://www.theguardian.com/technology/blog/2007/aug/19/adblockingis.

36. Noam Cohen, "Whiting Out the Ads, but at What Cost?," *The New York Times*, September 3, 2007, sec. Technology, accessed July 6, 2017, https://www.nytimes.com/2007/09/03/technology/03link.html.

"My argument is simple: blocking ads can be devastating to the sites you love," wrote *Ars Technica*'s Ken Fisher.[37] Fisher made the somewhat gentler case that blocking ads "can result in people losing their jobs, it can result in less content on any given site, and it definitely can affect the quality of content."[38] On *Destructoid,* Yanier Gonzalez noted that half of all of the site's readers blocked ads. He assured readers who used adblocking software that "we're still friends" but that adblocking practices mean that "we're working twice as hard as ever to sustain our company, as if keeping a group of game writers fed isn't difficult enough. We see gaming sites shut down or selling out so often these days."[39]

Both authors explained the lengths they went to in order to make sure that the ads presented to readers were as relevant and as unobtrusive as possible, and frequently tried to reassure the readers that they weren't taking an accusatory stance. However, whether intentionally or not, both writers obliquely referred to an Internet culture or mindset responsible for their readers choosing to reject the ad-supported publishing model despite the obvious consequences for their sites. Gonzalez stated that "(let's be honest) my Internet generation expects everything to be free, cheap, and plentiful," the presence of the possessive implying he was attempting to relate to this particular mindset.[40] Fisher had similar comments

37. Ken Fisher, "Why Ad Blocking Is Devastating to the Sites You Love," *Ars Technica*, March 6, 2010, accessed July 6, 2017, https://arstechnica.com/business/news/2010/03/why-ad-blocking-is-devastating-to-the-sites-you-love.ars.

38. Ibid.

39. Yanier Gonzalez, "Half of Destructoid's Readers Block Our Ads. Now What?," *Destructoid*, March 9, 2013, accessed July 6, 2017, https://www.destructoid.com/half-of-destructoid-s-readers-block-our-ads-now-what--247904.phtml.

40. Ibid.

about an Internet culture, saying that "I think in some ways the Internet and its vast anonymity feeds into a culture where many people do not think about the people, the families, the careers that go into producing a website." A more telling suggestion as to how the readers are perceived occurs further in the article, however. Recounting the dismal rate of people who chose to subscribe to the website following a short, 12-hour experiment where content on the site was hidden from users who blocked ads (for which the site receive a significant amount of negative feedback about its execution of the experiment), Fisher said, "we made the mistake of assuming that everyone who is blocking ads at Ars is doing so with malice."[41] This admission hardly fits with the earlier attempts at reassuring the readers that website owners understand their concerns over advertising. Both writers' perspectives suggest a relatively inflexible and simplistic assumption of the users' motivations. As I will discuss below, attempts at framing user reluctance to view ads as simply an issue of ads being "annoying" further emphasizes the disconnect from the users as well as an uncritical acceptance of the advertising revenue model on the part of these website owners.

**Acceptable Ads**

As early as 2009, Wladimir Palant, the current developer of Adblock Plus, indicated that he was somewhat sympathetic towards arguments on the ethical problems of ad blocking. In a blog post on the Adblock Plus site, Palant mused about the possibility of allowing a way for website owners who "[think] that the ads used on [their] site aren't intrusive" to display a small frame or banner

41. Fisher, "Why Ad Blocking Is Devastating to the Sites You Love."

requesting Adblock Plus users to whitelist the site, even offering the user the option to temporarily view the site with its full advertising enabled. Palant did acknowledge both his support of the user remaining ultimately in control and the danger of allowing website owners to make the decision, saying "if we allow webmasters to specify which ads the user should view or whether users with Adblock Plus should be allowed to visit their sites, they will try to maximize their profits—and very soon users will be confronted with intrusive ads everywhere or locked out of all sites."[42]

In 2011, however, Palant implemented a more substantial and long-reaching change in the Adblock Plus project. Calling the feature "Acceptable Ads," Palant reported that Adblock Plus would allow, by default, certain advertisements that were deemed "non-intrusive."[43] A page on the Adblock Plus website provided more detail on what was considered "acceptable advertising," providing strict limits on the amount of the whole page that advertising could occupy as well as prohibiting certain obnoxious features such as ads that played sound or video, loaded new advertising content, and expanded or otherwise changed shape as the user browsed the webpage.[44] This page also details on how Adblock Plus profits from the Acceptable Ads program, claiming that the advertising providers are only charged a fee if they achieve a certain number of ad views, in which case "our

42. Wladimir Palant, "An Approach to Fair Ad Blocking," *Adblock Plus and (a Little) More*, May 11, 2009, accessed July 11, 2017, https://adblockplus.org/blog/an-approach-to-fair-ad-blocking.

43. Palant, "Allowing Acceptable Ads in Adblock Plus."

44. "Allowing Acceptable Ads in Adblock Plus," *Adblock Plus*, accessed July 14, 2017, https://adblockplus.org/acceptable-ads.

licensing fee normally represents 30 percent of the additional revenue created by whitelisting its acceptable ads."[45]

At a technical level, the user could still opt to disable the whitelisting of acceptable ads, as the option was simply provided in the form of another filter list which allowed, rather than blocked, certain advertisements. Users who already subscribed to specific privacy-oriented filters would also not see acceptable ads displayed, but for all others—new users and users updating to the newest version of the software alike—their adblocking plugin would, instead of blocking advertisements, now allow advertisements deemed "acceptable," not by the users by themselves, but by the creator of the program who stood to profit from this decision.

This announcement was understandably a surprise to the users of the software, many of whom objected to the allowing of advertisements in general and the automatic enabling of the Acceptable Ads feature specifically. Commenting on Palant's original post, user Ninnit asked, "shouldn't you rename it 'This use [sic] to be a useful piece of software until I got paid by ad companies'? At least then it would be an accurate name as 'AdBlock' implies that it will block ads."[46] Most of the other comments on the blog announcement were generally positive towards the change, however, with users stating that they didn't mind supporting content online through advertising, but were concerned with

---

45. Ibid.

46. Ninnit, December 12, 2011 (02:58), comment on Wladimir Palant, "Allowing Acceptable Ads in Adblock Plus," *Adblock Plus and (a Little) More*, December 5, 2011, https://adblockplus.org/development-builds/allowin-acceptable-ads-in-adblock-plus.

obnoxious ads that played audio or video, or otherwise interrupted the browsing experience.

On the Adblock Plus forum, however, the reaction was substantially more negative. Many existing users were not happy that Adblock Plus enabled acceptable ads when the extension updated; while the installation and update tools do provide a notification that acceptable ads are enabled and offer the user an easy way to opt-out, many users thought the initiative should require users to opt-in to seeing advertisements, not be shown the ads by default. In an early forum post attempting to clarify some aspects of the initiative, Palant cited the appeasement of participating advertising companies as the rationale for both the sweeping change and the automatic opting-in of users:

> I feel with you and it wasn't an easy decision to make. However, this isn't something that can be rolled out gradually, to new users only. We got some companies interested, one of them even agreed to disable animations during the pilot phase to meet our requirements. If they notice that it isn't worth doing (only few Adblock Plus users have the feature enabled) they will go back to more annoying ways of advertising because that's where the money is right now.[47]

Many users were concerned with the situation that the acceptable ads initiative placed Adblock Plus in—on the one hand, the software was ostensibly designed to block advertisements for users, but now that purpose was balanced with the providing favorable conditions for advertisers interested in having their ads allowed by the plugin. User Antoviaque commented on a possible conflict of

---

47. Wladimir Palant, "Re: Allowing Acceptable Ads in Adblock Plus," *Adblock Plus*, December 5, 2011, accessed July 14, 2017, https://adblockplus.org/forum/viewtopic.php?p=52838#p52838.

interest in the future, saying, “I think you'll agree that, as the revenues from advertisers grow, it will create pressure on the project that won't always be aligned with the users' interests. AdBlock can resist those pressures, but history has shown that ad-driven businesses often have to do compromises that are detrimental to their user-base.”[48] Others saw the move as actively hostile to the user, and stated that they would be switching to other adblocking programs that did not compromise on functionality. “I decided to switch ad blocking to software you don't control. Once software gets away with attacking the user like yours has done, more is probably in the pipeline,” wrote user DaemonFC.[49] Regardless of the concerns of users commenting on the blog post and forums, Adblock Plus’ popularity does not seem to have been affected by the Acceptable Ads initiative, as it remains the most popular extension on Mozilla’s centralized collection of extensions for Firefox with over 15 million users,[50] as well as on the Chrome Store for extensions to Google’s Chrome browser, where it has over 10 million users.[51]

48. Xavier Antoviaque, “Re: Allowing Acceptable Ads in Adblock Plus,” *Adblock Plus*, December 12, 2011, accessed July 14, 2017, https://adblockplus.org/forum/viewtopic.php?f=1&t=8872&start=30#p53180.

49. DaemonFC, “Re: Allowing Acceptable Ads in Adblock Plus,” *Adblock Plus*, December 12, 2011, accessed July 14, 2017, https://adblockplus.org/forum/viewtopic.php?f=1&t=8872&sid=f1b1ddfd3237ac059928b22bbd035b82&start=15#p53134.

50. “Adblock Plus :: Add-Ons for Firefox,” last modified June 7, 2017, accessed July 14, 2017, https://addons.mozilla.org/en-US/firefox/addon/adblock-plus/.

51. “Adblock Plus - Chrome Web Store,” *Chrome Web Store*, last modified July 12, 2017, accessed July 14, 2017, https://chrome.google.com/webstore/detail/adblock-plus/cfhdojbkjhnklbpkdaibdccddilifddb.

## Obligatory Ads

Dallas Smythe theorized the idea of the audience commodity as the work done by audiences of nominally "free" traditional mass media, such as broadcast television, in the form of attention and receptiveness to advertising—"learning to buy goods and to spend their income accordingly."[52] In the case of online advertising, the users are even more ensnared in this particular economic mode; while Smythe questioned the audience obligation in the context of a television left on but unattended in an adjacent room, the Internet user has neither the ignorance of this particular economic arrangement nor—without the aid of tools like adblocking software—the ability to figuratively step into the other room during a commercial break. So thoroughly integrated into the online experience is advertising—and its component surveillance—that the advertising model enjoys a near absolute hegemony over online life that is reflected in the very discourse over advertising. As with discourses of piracy, when website owners speak of viewing a website's content without the corresponding advertisements as "theft," they are already framing the discussion in terms amenable to this particular ideology: the user is intended to either view the website with its ads (and be tracked), or the user has no right to access this freely-available site in the first place. Fisher of Ars Technica stated this expectation in fairly concrete terms: "if a site has advertising you don't agree with, don't go there. I think it is far better to vote with page views than to show up and consume resources without giving

52. Dallas Smythe, "On the Audience Commodity and Its Work," in *Media and Cultural Studies: Keyworks*, ed. Meenakshi Gigi Durham and Douglas M. Kellner, 2nd ed. (Malden, MA: Blackwell Publishing, 2009), 243.

anything in return," and waved off user concerns that advertising is a flawed business model by saying, "my response is simple: either you care about the site's well-being, or you don't."[53] Any discussions of whether that sort of one-sided agreement made after the fact is valid are entirely pre-empted in framing the user as a law-abiding (online) citizen or a thief. Smythe referred to the programming that accompanies advertising as the "free lunch" that the audiences receive in return for their attention; the free lunch "must always be subordinated to [the characteristics] of the formal advertisements,"[54] but in the case of the Internet the creators of the "free lunch" have incredibly taken up haranguing audiences for their lack of attention, placing an even greater focus on the economics of advertising that control the entire system. And in a textbook example of the normalization of an ideological framework, the most problematic aspect of this arrangement is the total complicity of the user within this rhetoric. Zuckerman said that "we've been taught that this is simply how the Internet works: if we open ourselves to ever-increasing surveillance—whether from corporations or governments—the tools and content we want will remain free of cost."[55]

This sentiment—that the user's role is in the unquestioning acceptance of the economic structures of the web—is echoed surprisingly frequently by people who nominally sympathize with the plight of the users—or even by the users

---

53. Fisher, "Why Ad Blocking Is Devastating to the Sites You Love."

54. Smythe, "On the Audience Commodity and Its Work," 242.

55. Zuckerman, "The Internet's Original Sin."

themselves. Responding to complaints about the Acceptable Ads initiative in the Adblock Plus forum, user RedneckBabe wrote:

> Quite a few in here, who regularly cheat content creators out of money, screaming 'bout betrayal, extortion, morals and ethics….Maybe you should do a gut check, each month send money to all websites that you've betrayed and cheated out of income, and help eliminate the need for ads all together. Maybe a group of you upstanding net citizens could help eliminate all advertising on the internet by actually paying for the content you consume.[56]

In a much less blunt fashion, Gonzalez of Destructoid attempted to strike a sympathetic pose in exhorting his readers to not block ads on the site, but—whether accidentally or intentionally—he consistently frames ads as a simple annoyance, downplaying or ignoring entirely user concerns about privacy. "Chances are...you understand that blocking ads denies us some coffers and you probably feel a little bad about it, but all ads intrinsically annoy you," before arguing that the website does its best to refuse ads that expand over text, play audio or video, or otherwise cosmetically interrupt user's browsing.[57] To the extent that users concerned about their privacy are addressed, Gonzalez dismisses them as irrational ideologues: "there are plenty of Internet users who hate ads on principle or want ultimate non-tracking privacy [and who will] eventually just use a different adblocker that doesn't have a whitelist policy....Some people are above appeals, no matter how much we bend the advertising industry."[58] When site

---

56. RedneckBabe, "Re: Allowing Acceptable Ads in Adblock Plus," *Adblock Plus*, December 12, 2011, accessed July 14, 2017, https://adblockplus.org/forum/viewtopic.php?f=1&t=8872&start=30#p53199.

57. Gonzalez, "Half of Destructoid's Readers Block Our Ads. Now What?"

58. Ibid.

owners or content creators ask users to disable adblocking software and either ignore or belittle privacy concerns, they send the clear message that the user's concern over privacy issues comes second to the *right* of websites to make money through this particular economic model. In other words, they are either unaware (unlikely) or do not care that their means of revenue is hostile to the users. Where this becomes especially problematic is the fact that very few websites—and certainly no sites the size of Ars Technica or Destructoid—handle their own advertising directly, instead relying on large networks to both sell and place ads on their behalf. Website owners are all too willing to receive advertising revenue —and defend their use of the business model—but at the same time they wash their hands of the responsibility of ensuring that the advertising they feature on their sites is not actively hostile to the users. The website has no responsibility for when something goes wrong—a poorly-vetted ad becomes a vector for malware, or user data collected through these advertising and tracking initiatives is exposed online, for example. In their appeals to disable adblocking, both Gonzalez and Fisher admitted that advertising is out of their control despite best efforts. Gonzales claimed that Destructoid does not allow ads that play audio or change shape, but reminded users to contact him if they ever did see such ads on the site (a seemingly unnecessary caveat if the site truly does not accept those kinds of ads in the first place) and went on to defend the use of Flash ads (a format which is responsible for more sophisticated methods of tracking such as the zombie cookie) as more profitable than less-intrusive static or animated banners.[59] Fisher

59. Ibid.

claimed that “over 12 years…we will fight on the behalf of readers whenever we can. Does that mean that there are the occasional intrusive ads, expanding this way and that? Yes, sometimes we have to accept those ads.”[60]

“We have to accept those ads.” Fisher does not go into further detail on why this is not negotiable—is the site unable to choose what types of advertisements it receives from the ad network? Will advertising be pulled entirely if a website attempts to negotiate the types of ads featured?—but the implication is clear: if the website is to feature advertisements as its main source of revenue, then the desires of the user will ultimately be a secondary consideration.

**Conclusion**

The Acceptable Ads initiative from Adblock Plus makes two assumptions about the user: the first is that the user is willing to view ads as long as the ads adhere to certain standards of display and formatting, and the second is that, despite whitelisting functionality being built into Adblock Plus (all adblocking software features the ability to un-block ads for certain websites) the user is not competent or able to make exceptions for sites they wish to support. Substantial criteria for what constitutes an acceptable ad focuses entirely on the visual dimensions of the advertisement on the webpage itself, with heavy emphasis on weeding out “annoying” or “intrusive” content. What is not covered in the policy is the underlying code of the advertisement that tracks a user’s actions across the

60. Fisher, “Why Ad Blocking Is Devastating to the Sites You Love.”

Internet. If a user is simply concerned about seeing too many advertisements, or possibly having their web browsing slowed by the presence of large, bandwidth-heavy advertisements, this is certainly an acceptable compromise. For users who installed Adblock Plus in order to forcefully "opt-out" of online tracking and attempt to regain a modicum of control and agency in their online experience, however, this initiative accomplishes nothing, and Adblock Plus becomes yet another series of middlemen whose revenue comes at the expense of the user.

In the advertising-supported ecosystem of the modern Internet, the user is product first and customer second—and while online advertising ostensibly shares the goal of all advertising—that is, to compel the viewer to purchase or use a specific product or service—it would not be ridiculous to ask whether the user-as-consumer has become simply a vestigial part of this entire ecosystem, where the true revenue resides in the infinite trading of user data and refinement of the processes of collection. The user has no negotiating power within this system beyond the glib and disingenuous suggestions that they can just avoid using websites if they don't support advertising. In this entirely powerless existence, the use of adblocking software is an act of resistance against a "social contract" to which the user has not agreed but is expected to be a willing and enthusiastic participant in. In protecting themselves from the pervasive tracking and exploitation of personal data for profit that has become the underlying structure of the Internet, the user also rejects the advertising industry's assertions that the user has a moral and ethical obligation to view ads as though it were part of some

sort of equal, negotiated economic exchange. The adblocking user also rejects the lack of vision of website owners who produce content which they feel has monetary value and that they should be compensated for, but lack the creativity or concern to find a revenue model to support their work that does not depend on the exploitation of other users (though website owners and content creators are, ironically, users themselves and subject to the same intrusions that constitute their prime source of revenue). Most importantly, the adblocking user implicitly but completely rejects the hegemonic assumption that the mere existence of the online advertising model compels their support of and obedience to the industry's practices.

# CHAPTER VI

# CASE STUDY III: THE USER IS VISIBLE—THE KILTON PUBLIC LIBRARY AND THE TOR ANONYMITY NETWORK

## Introduction

The previous two case studies concerned specific events and technologies which have contributed to the present shape of the Internet where the user is a disempowered, alienated commodity figure. This figure has been removed from a place at the center of the logic of the Internet and instead had been exiled to the periphery, moving through the network only in ways sanctioned by entities which have an economic interest in the user adhering to certain patterns. This chapter will discuss a privacy-oriented software tool called Tor, which allows the user to browse the Internet anonymously. Much like the ad-blocking software discussed in the last chapter, Tor and similar anonymity tools allow the user to reclaim some of the agency and autonomy that has been denied them under the Californian ideology which orders the online space. Understandably, organizations which have a strong economic or security interest in constantly knowing the user's whereabouts and activities would certainly be opposed to the creation and use of such tools.

While ad-blocking software represents a high-profile threat to the advertising industry's control of the Internet, the use of anonymity software is not often discussed as a problem worth addressing in that context. Instead, anonymity software puts the privacy-conscious user in conflict with the state itself,

particularly in light of the 2013 revelations by former NSA contractor Edward Snowden which detailed the extent of the National Security Agency's international surveillance programs. While the user may indeed rely on anonymity tools to avoid the tracking and profiling practices of the advertising industry, the opposition to the user's access comes from a far larger, more powerful, and less-transparent adversary.

The focus of this chapter concerns a pilot program which was run at a the Kilton Public Library in West Lebanon, New Hampshire in 2015. In keeping with the general ideological nature of the public library as an egalitarian place of free, democratized access to information, this particular library participated in the Tor network by serving as a relay of anonymous traffic. Citing the potential for criminal misuse, law-enforcement authorities at both the local and national level put subtle—and unofficial—pressure on the library to cease its involvement with the project. This example will be part of a wider discussion of the frequent rhetorical tactic on the part of law enforcement and intelligence agencies which attempts to link practices of anonymity with criminal activity.

## A Brief History of Tor

Before discussing the case of the Kilton Library, it is important to briefly explain how Tor functions. The name "Tor" was initially styled "TOR," an acronym for "the onion router" in a nod to the technology behind it.[1] Tor allows users to anonymously surf the Internet through a network architecture called

1. "Why Is It Called Tor?," *Tor Project: FAQ*, accessed July 14, 2017, https://www.torproject.org/docs/faq#WhyCalledTor.

"onion routing," developed as a project at the U. S. Naval Research Laboratory and first presented in a workshop paper by David Goldschlag, Michael Reed, and Paul Syverson in 1996.[2] The authors were concerned with the security of online communications for military applications; while the use of encryption allows for communicating parties to keep the content of their messages private, unwanted third parties can still confirm that communication is taking place, potentially identify the participants, and make inferences as to the context based on that knowledge in what is called traffic analysis.[3]

Onion routing protects against traffic analysis in addition to hiding message content by first passing all communications through an encrypted series of routers, or nodes, connected together in a virtual network. The nodes are all permanently connected to each other and have knowledge of all other possible nodes in network, but when a user first opens a connection to an onion network a specific path or circuit is mapped through the network by the user's computer. The circuit changes each time a user connects to the service, so there is no predictable path that a user's data will take through the onion network, even though the actual nodes remain relatively unchanged.[4] Once a circuit has been created, data is sent through the circuit in a structure called an onion. The onion

2. David M. Goldschlag, Michael G. Reed, and Paul F. Syverson, "Hiding Routing Information," in *Information Hiding*, Lecture Notes in Computer Science (presented at the International Workshop on Information Hiding, Cambridge, UK: Springer, 1996), 137–150, http://dx.doi.org/10.1007/3-540-61996-8_37.

3. Michael G. Reed, Paul F. Syverson, and David M. Goldschlag, "Anonymous Connections and Onion Routing," *IEEE Journal on Selected Areas in Communications* 16, no. 4 (May 1998): 482.

4. Goldschlag, Reed, and Syverson, "Hiding Routing Information," 142.

is composed of the actual data packets to be transmitted which are wrapped in sequential layers of encryption corresponding to the different nodes within the circuit. These layers also contain information about the previous and next nodes in the circuit, so as an onion passes through the networks, the individual nodes are only able to immediately identify the node from which they received the onion, and the node to which they are sending it. As the onion passes through each node, the corresponding encryption layer is stripped off—much like peeling layers from an onion—until the raw data arrives at its destination.[5]

One of the most notable features of onion routing is that it works at the application layer of the Internet protocol suite[6]—that is, the onion routing network is a virtual network which requires no special changes to the physical infrastructure of the Internet or bespoke configuration of the user's computer. As onion routing technically functions as a proxy network, many existing applications can be directed to pass their data through the onion routing network for increased privacy and anonymity, again with no requirements that the applications themselves are specifically aware of this configuration. The most common use of onion routing is to anonymize a user's web browsing, but the protocol supports a variety of other uses, including a providing secure channel for chat programs, email, and even logging into remote computer systems to access files or perform

5. Ibid., 140–141.

6. R. Braden, ed., "Requirements for Internet Hosts - Communication Layers," *Internet Engineering Task Force* RFC1122 (October 1989), accessed June 4, 2016, http://dx.doi.org/10.17487/RFC1122.

tasks.[7]

Much in the same way that the ARPANET project was the result of collaboration between military interests and civilian researchers, onion routing technology was developed on behalf of the U. S. Navy (with later DARPA involvement)[8] but was of great interest to non-military computer and security researchers. The Tor Project began in 2002, when Syverson joined Roger Dingledyne in implementing the results of the Naval research to develop a free, open onion routing network that they called Tor (TOR). Tor was still actively funded by the Navy at the time, but the resulting software and source code was made available to computing enthusiasts interested in onion routing technology. The Tor Project debuted an early alpha version on September 20th, 2002.[9] Dingledyne, Nick Mathewson, and Syverson presented a paper at the USENIX Security Symposium in 2004 detailing the changes that Tor made to previous generations of onion routing, the experience with the limited global number of Tor nodes at the time, and some active security concerns facing the use of anonymous communication online. One specific—though by no means the only—issue was the potential ability for the Tor network to be used to hide the identities of spammers or criminals using the anonymity of the network to launch attacks

7. Reed, Syverson, and Goldschlag, "Anonymous Connections and Onion Routing," 489–491.

8. Paul Syverson, "Our Sponsors," *Onion Routing*, last modified 2005, accessed July 20, 2017, https://www.onion-router.net/Sponsors.html.

9. Roger Dingledine, "Pre-Alpha: Run an Onion Proxy Now!," last modified September 20, 2002, accessed July 13, 2017, http://archives.seul.org/or/dev/Sep-2002/msg00019.html.

against websites.[10] This concern has continued to this day and is quite relevant in the discourses concerning Tor in the context of this case study.

### The Kilton Public Library

The Library Freedom Project, according to its webpage, is "a partnership among librarians, technologists, attorneys, and privacy advocates which aims to address the problems of surveillance by making real the promise of intellectual freedom in libraries."[11] In keeping with that goal, the LFP developed an initiative in collaboration with the Tor Project that sought to convince public libraries to run Tor nodes as a library service, which would help increase the size—and therefore, the anonymity and robustness—of the global Tor network.[12] The project would initially see participating libraries simply hosting a middle relay to pass data traffic along inside the Tor network, with the ultimate goal being that the libraries would host an exit node, or a relay where traffic would exit the network. Any Tor users who were browsing with a network circuit built with the a public library as the exit relay would appear to be browsing from that library itself.

The Kilton Public Library in West Lebanon, New Hampshire was the first library to volunteer to participate in this initiative. This happened in part as a result of the IT librarian's familiarity with privacy software and his past decision

10. Roger Dingledine, Nick Mathewson, and Paul Syverson, "Tor: The Second-Generation Onion Router," in *Proceedings of the 13th USENIX Security Symposium* (presented at the 13th USENIX Security Symposium, San Diego, CA: The USENIX Association, 2004), 312, https://www.usenix.org/conference/13th-usenix-security-symposium/tor-second-generation-onion-router.

11. "What Is the Library Freedom Project?," *Library Freedom Project*, n.d., accessed July 20, 2017, https://libraryfreedomproject.org/.

12. Alison Macrina and Nima Fatemi, "Tor Exit Relays in Libraries: A New LFP Project," *Library Freedom Project*, n.d., https://libraryfreedomproject.org/torexitpilotphase1/.

to migrate the library's computer systems to the Linux operating system, which is not only considerably more secure than the usual Windows-based systems found in most library settings but also allows for easier and more in-depth configuration as a Tor relay.[13] Library Freedom Project director Alison Macrina had given a presentation on computer privacy at the library in May 2015, and discussed the project with librarians at that time. The library's board of trustees approved the proposal, and the middle relay at the Kilton Public Library went online in July, 2015.[14] Technology blog Ars Technica wrote a brief news report about the relay which strongly focused on the overall privacy-oriented aim of the Library Freedom Project. The report did mention that, at the time, the Kilton library's Tor relay was a middle relay only, meaning that it passed traffic along through the Tor network but did not deliver any data between Tor and the unsecured Internet.[15] Shortly after the relay had been brought online, however, it was shut down by the library administration. Officials from the United States Department of Homeland Security learned of the library's plan to run a Tor relay through the Ars Technica article[16] and brought the plan to the attention of the Lebanon Police Department, which in

13. Ibid.

14. Julia Angwin, "First Library to Support Tor Anonymous Internet Browsing Effort Stops After DHS Email," *ProPublica*, last modified September 10, 2015, accessed October 14, 2015, https://www.propublica.org/article/library-support-anonymous-internet-browsing-effort-stops-after-dhs-email.

15. Cyrus Farivar, "Crypto Activists Announce Vision for Tor Exit Relay in Every Library," *Ars Technica*, last modified July 30, 2015, accessed July 13, 2017, https://arstechnica.com/tech-policy/2015/07/crypto-activists-announce-vision-for-tor-exit-relay-in-every-library/.

16. Cyrus Farivar, "Library's Tor Relay—which Had Been Pulled after Feds Noticed—now Restored," *Ars Technica*, last modified September 16, 2015, accessed July 13, 2017, https://arstechnica.com/tech-policy/2015/09/small-town-library-restores-tor-relay-which-had-gone-dark-for-weeks/.

turn met with city officials and library administration to warn of Tor's potential to facilitate criminal activity.[17] At no point did either the Department of Homeland Security or the Lebanon Police Department formally prohibit the library from running the node or open any kind of investigation—a representative of the DHS was quoted as only wanting to provide "situational awareness," and a lieutenant at LPD similarly "felt we needed to make the city aware of it."[18] However, given the concerns of local law enforcement, the Lebanon library director voluntarily turned off the relay to allow for further discussion about the technology among the library board, the city, and the public.

The announcement of the closure of the Tor relay was met with a substantial amount of interest online, with many technology news sites commenting critically on the unusual role of the Department of Homeland Security in the events. A number of activist organizations, including the Library Freedom Project, the Freedom of the Press Foundation, the Electronic Frontier Foundation, the American Civil Liberties Union, and the Tor Project itself joined together in writing an open letter to the library explaining the legitimate uses of Tor and its importance to free online expression.[19] The EFF created an online petition allowing Internet users to indicate their support for the Tor relay to the

17. Angwin, "First Library to Support Tor Anonymous Internet Browsing Effort Stops After DHS Email."

18. Ibid.

19. See https://libraryfreedomproject.org/wp-content/uploads/2015/09/Kilton-Letter.pdf.

Kilton library board.[20] The petition gathered over 4,300 signatures; by comparison, the city of Lebanon has a population of a little over 13,000 people as of the 2010 U. S. Census. The local newspaper, the *Valley News*, also spoke up in support of the initiative in a staff editorial, stating that "even as we concede that a deep understanding of global encryption technology is above our pay grade, we applaud the Kilton Public Library staff for taking the lead in a suddenly controversial project that supports anonymous web surfing."[21]

The Kilton Library Board of Trustees held a vote at a meeting on September 15th, and on the 16th, the *Valley News* reported that the Tor relay in the Kilton library would be reactivated following substantial support from the community and other interested parties at the meeting.[22] A news report the following week published the results of the ACLU's request for information on the email chain that started the controversy. On August 5th, less than a week after the Ars Technica article on the Library Freedom Project, Special Agent Gregory Squire of the Department of Homeland Security in Boston forwarded the Ars Technica article on the Kilton Library's Tor relay to Detective Sgt. Tom Grella, in Portsmouth, NH; notably, Grella headed up the state's Internet Crimes Against Children Task Force. In Squire's email, the forwarded article was accompanied by

20. "Support Tor and Intellectual Freedom in Libraries," *EFF Action Center*, accessed July 13, 2017, https://act.eff.org/action/support-tor-and-intellectual-freedom-in-libraries.

21. Staff, "Editorial: Privacy Concerns and the Kilton Library," *Valley News* (West Lebanon, NH, September 15, 2015), sec. Opinion, accessed July 21, 2017, http://mobile.vnews.com/Archives/2015/09/edit-tor-vn-091515.

22. Nora Doyle-Burr, "Despite Law Enforcement Concerns, Lebanon Board Will Reactivate Privacy Network Tor at Kilton Library," *Valley News* (West Lebanon, NH, September 16, 2015), accessed October 14, 2015, http://www.vnews.com/home/18620952-95/library-joins-privacy-network.

a single line of text: “just terrific … that kid [Macrina] seems to be thinking just an inch past the end of her nose.”[23] Grella then forwarded the article to Sgt. Richard Norris of the Lebanon police, who was the one to discuss law enforcement concerns with the library.

**Criminalizing Anonymity**

Put very broadly, Tor is a tool that protects against the conditions discussed in the previous two chapters. The Internet user—if they want to be an active user—is always required to be verified, and is always tracked. In other words, the user is always in a persistent state of visibility. Ad-blocking can help mitigate this with regards to the pervasive tracking of the user by commercial interests, but the all-consuming nature of online surveillance at the hands of the state renders such tools ineffective for these purposes. Tor resists and complicates the electronic eye of the state first and foremost; while it certainly enables the user to “opt-out” of the tracking and verification imposed by the commercial Internet, using Tor for that purpose alone is somewhat excessive given its capabilities, and is rarely included in the same discussions as adblocking technologies.

However, the use of Tor and ad-blocking software do have one thing in common: both are the object of discursive practices which seek to discredit, stigmatize, and ultimately criminalize the user who employs these technologies. And as with ad-blocking, the fundamental terms of this discourse are imposed by

---

23. Nora Doyle-Burr, “Emails Describe DHS Tor Concern,” *Valley News* (West Lebanon, NH, September 27, 2015), accessed October 15, 2015, http://www.vnews.com/news/18760917-95/emails-describe-dhs-tor-concern.

power—in this case, the power of the state, not capital—and as such the user is almost entirely powerless to contest them. The discourses which criminalize ad-blocking or online anonymity act, in Foucauldian terms, as disciplinary measures aimed at producing the predictable, traceable, and visible Internet user—the docile digital body. Speaking of Bentham's model of the panopticon, Foucault observes that "the perfect disciplinary apparatus would make it possible for a single gaze to see everything constantly."[24] In the current climate of perpetual state surveillance, is not such an apparatus already possible (albeit not in the human sense Foucault was no doubt envisioning)? And for a tool like Tor to confound that kind of observation must pose a nearly indescribable threat to entities that consider perfect knowledge of all online communications a non-negotiable part of their work. Material released by Edward Snowden disclosing the extent of the National Security Agency's surveillance programs indicated that the agency had been entirely unsuccessful in breaking Tor's security.[25] In a leaked NSA presentation entitled, "Tor Stinks," the first slide states the situation clearly: "we will never be able to de-anonymize all Tor users all the time."[26] The presentation emphasized the importance of and relative success through other potential attacks against Tor users which attempted to exploit human error or

24. Michel Foucault, *Discipline & Punish: The Birth of the Prison* (New York, NY: Vintage Books, 1977), 173.

25. James Ball, Bruce Schneier, and Glenn Greenwald, "NSA and GCHQ Target Tor Network That Protects Anonymity of Web Users," *The Guardian*, October 4, 2013, sec. US news, http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption.

26. National Security Agency, "Tor Stinks," *Electronic Frontier Foundation*, last modified October 4, 2013, https://www.eff.org/document/2013-10-04-guard-tor-stinks.

poor security practices as a means of eavesdropping on communications through the network.

And it isn't just American intelligence agencies that are stymied by the security offered by Tor. Over a period of about eight months in 2012 and 2013, a Japanese man named Yuusuke Katayama made a number of anonymous bomb and death threats online, directed at government buildings and officials, corporate headquarters, and public spaces. Katayama was eventually apprehended, but his advanced knowledge of Internet security allowed him to gain remote access to the computers of unrelated strangers to make his threats look as though they originated from those machines. Following Katayama's arrest, the National Police Agency suggested strongly to Internet service providers that they block the use of Tor entirely to prevent future such incidents. The NPA would have had to obtain a warrant in order to officially restrict all Tor and other anonymous Internet traffic, but by applying subtle, firm—yet entirely unofficial—pressure to ISPs to address the issue from their perspective, law enforcement could attempt to achieve the same results without having to navigate potential accusations of censorship.[27]

Given that no actual or even suspected criminal activity emerged as a result of the Kilton Public Library's Tor relay, the reaction of law enforcement and intelligence officials seems entirely disproportionate. But it also provides a glimpse into the state's approach to online anonymity. That the Department of Homeland Security itself was involved certainly speaks to the seriousness with

27. Christopher St. Louis, "For Your Protection: State Surveillance and Narratives of Risk in Contemporary Japan" (Master's Thesis, University of Tokyo, 2014), 52–54.

which intelligence agencies treat the problem posed by Tor. And the highly visible initial point of contact with the DHS—a state law enforcement official who heads up the task force that addresses the trafficking of child pornography over the Internet—strongly signals the preferred weapon against users who would pursue anonymity online: the implication of guilt through (largely fictional) association.

Some of the most persistent narratives around Tor involve hidden services —websites which can only be connected to through the Tor network, and which are more commonly referred to as "the dark web."[28] There are entirely legitimate uses for hidden services on the dark web. News outlets like *The Guardian*[29] and *The Intercept*[30] use hidden services as a way to allow whistleblowers to submit critical information securely and anonymously. Independent journalism organization *ProPublica* offers a version of its website via a Tor hidden service for readers in areas where some of its covered topics might be restricted.[31] As a lighter example, electronic artist Richard D. James—known by his stage name Aphex Twin—announced the release details and track listing of his most recent

28. Though "dark web" and "deep web" are sometimes used interchangeably, the definitions are entirely different. "Dark web" refers to websites and services only accessible through virtual networks like Tor, while the "deep web" refers to the substantial number of webpages and other data not immediately accessible through search engines.

29. "The Guardian SecureDrop Server," *The Guardian*, accessed July 13, 2017, https://securedrop.theguardian.com/.

30. "The Intercept Welcomes Whistleblowers," *The Intercept*, accessed July 13, 2017, https://theintercept.com/source/.

31Mike Tigas, "A More Secure and Anonymous ProPublica Using Tor Hidden Services," *ProPublica*, last modified January 13, 2016, https://www.propublica.org/nerds/item/a-more-secure-and-anonymous-propublica-using-tor-hidden-services.

album in 2014 via a mini website only accessible as a hidden service.[32]

This is not to say that criminal activity does not happen on the dark web. The 2013 closure of the Silk Road drug market was the result of the most high-profile law enforcement action on the dark web at the time, which shut down a black-market drug trade that was estimated to have served over 100,000 people.[33] A year later, the high profile "Operation Onymous" saw the FBI cooperating with Europol in an international bust that seized dozens of hidden service websites—including the "Silk Road 2.0"—selling drug, weapons, stolen credit cards and more.[34] But the characterization of the dark web as an exclusive repository of the most chilling illegal content or a gateway to the online criminal underworld may be substantially exaggerating the prevalence of that sort of activity. Researchers at Terbium Labs, a security firm that specializes in the dark web, conducted a survey of hidden service websites and found that nearly half of the content was entirely legal, with an additional 1/8 of sites being permanently offline. Of the illegal content represented in their survey, marketplaces for drugs comprised the majority of the sites at just under half, with legal (though likely not legally distributed) pornography and pharmaceutical drugs representing the next highest

32. Tim Jonze, "Aphex Twin Announces New Album SYRO via the Deep Web," *The Guardian*, August 18, 2014, sec. Music, http://www.theguardian.com/music/2014/aug/18/aphex-twin-announces-new-album-syro-via-the-deep-web.

33. Joseph Goldstein, "Arrest in U.S. Shuts Down a Black Market for Narcotics," *The New York Times*, October 2, 2013, sec. N.Y. / Region, https://www.nytimes.com/2013/10/03/nyregion/operator-of-online-market-for-illegal-drugs-is-charged-fbi-says.html.

34. Benjamin Weiser and Doreen Carvajal, "International Raids Target Sites Selling Contraband on the 'Dark Web,'" *The New York Times*, November 7, 2014, sec. Europe, https://www.nytimes.com/2014/11/08/world/europe/dark-market-websites-operation-onymous.html.

uses.[35] A less rigorous investigation conducted by a writer at Gizmodo found that, beyond activist sites or illegal marketplaces, much of the dark web "mostly resembles the internet of 20 years ago," with sites featuring such design elements as "a single word on a blank page. A stupid gif with autoplaying sound, an annoying trend that mostly died with Myspace."[36] And in an effort to verify one of the most persistently chilling rumors about the dark web—that it is even possible to arrange assassinations internationally at specialized hidden service websites—Motherboard found that one of the most professional, highly-regarded sites claiming to offer such services was simply a very thorough scam (albeit one with possible ties to organized crime).[37] All of this goes to argue that, while not entirely free of criminal activity, the hidden services of the Tor network are simply much more banal than most depictions imply—and may possibly not be much more transgressive than what can be found by motivated seekers in the clear Internet.

However, the discursive tactics employed by law enforcement and intelligence agencies seek to depict any use of Tor as tantamount to an admission of criminal intent. Caught in the center of this conundrum is the figure of the user: while anonymity technologies such as Tor present a powerful tool of resistance against the state of surveillance capitalism that governs the Internet,

35. Clare Gollnick and Emily Wilson, *The Truth About the Dark Web: Separating Fact from the Fiction*, White Paper (Terbium Labs, 2016), 8–14, https://terbiumlabs.com/darkwebstudy.html.

36. Bryan Menegus, "The Dark Web Is Mostly Full of Garbage," *Gizmodo*, last modified September 21, 2016, accessed November 8, 2016, http://gizmodo.com/the-deep-web-is-mostly-full-of-garbage-1786857267.

37. Joseph Cox, "This Fake Hitman Site Is the Most Elaborate, Twisted Dark Web Scam Yet," *Motherboard*, last modified May 18, 2016, https://motherboard.vice.com/en_us/article/mg77bn/this-fake-hitman-site-is-the-most-elaborate-twisted-dark-web-scam-yet.

and while they allow for the user to escape from the sort of all-encompassing tracking employed by the advertising industry, the anonymous user is always depicted as a guilty party with something to hide. Persistent narratives about the unequivocally criminal nature of anonymizing technology—and its users—produce a chilling effect calculated to keep the average user from considering the use of tools like Tor. If the suggestion of criminality-by-association wasn't enough, further analysis of documents released by Snowden found that, according to the rules in the filtering software run by the NSA to decide what Internet traffic to save for later analysis, simply conducting a search for information related to Tor or visiting the Tor Project website was enough to have a user's Internet traffic flagged for closer inspection.[38] These discursive practices are intended to make the user doubt the need for privacy tools in their life or worry about whether the search for certain kinds of information would open them up to additional scrutiny by law enforcement, in the arrangement theorized by Foucault: the panoptic disciplinary force that may or may not be watching, but nonetheless compels the subject to remain always on their best, most law-abiding behavior.[39] As the surveillance state is constantly asking the privacy-concerned subject: if you have nothing to hide, why would you try to hide in the first place? For the purposes of the state, if it cannot defeat the security provided by technologies such as Tor, then the next best option is to ensure as few people as possible actually use it.

38. Jacob Applebaum et al., "NSA Targets the Privacy-Conscious," last modified July 3, 2014, accessed July 13, 2017, http://daserste.ndr.de/panorama/aktuell/NSA-targets-the-privacy-conscious,nsa230.html.

39. Foucault, *Discipline & Punish*, 201–202.

## Conclusion

From the outset, Tor is not easy software to run. Though the Tor Project provides a mostly-preconfigured web browser to download that handles all of the work of creating a new circuit through the network, the concept behind onion routing is somewhat complicated, and the average user may not understand how it benefits them. In spite of Tor's relative lack of general popularity and in spite of the Kilton Public Library initially only providing a middle relay in a town of 13,000 people, agents with the Department of Homeland Security felt compelled to intervene—not through any sort of active policing action but to cast doubt on the legality and legitimacy of the project. A spokesman with the Department of Homeland Security told Ars Technica that

> [Homeland Security Investigation] does not make policy determinations for local communities, but rather chooses to focus on the criminal investigations of transnational crime, which would include cyber-enabled offenses. The use of a Tor browser is not, in and of itself, illegal….However, the protections that Tor offers can be attractive to criminal enterprises or actors and HSI will continue to pursue those individuals who seek to use the anonymizing technology to further their illicit activity.[40]

The somewhat disingenuous protestation of innocence does not acknowledge the obvious chilling effect the interest of such a government agency would have on the project and the people associated with it. But this also makes a tentative argument for the seriousness with which the surveillance state takes the issue of tools like Tor. Ironically, the tools that would allow the Internet user to regain their agency and privacy, and opt-out of the surveillance capitalism that governs

40. Farivar, "Library's Tor Relay—which Had Been Pulled after Feds Noticed—now Restored."

the Internet, will also see the user branded a person of suspicion and a potential criminal. When the entire structure of the Internet is currently developed around promoting and maintaining the visibility of the docile body of the user, negating that visibility is to, in a way, reject prescribed modes of participation in the Internet itself. This possibility is of course completely unacceptable to the entities which benefit from the current structures of power online, but if the user is to be reinstated as the active subjectivity at the center of the Internet, this kind of radical contestation of the established ordering logic may the first step in reclaiming that lost legacy.

# CHAPTER VII

# CONCLUSION

## One More Example

The modern Internet is far richer in content than could have possibly been imagined in 1995. Every conceivable interest or hobby (no matter how legal) is represented online and can be unearthed with a little digging or—increasingly—knowledge of the proper Google search terms. In my own aimless online wanderings of the week this chapter was written, I can consciously recall visiting micro-communities in specialized forums dedicated to topics such as functionally minimal aesthetic configurations of graphical user interfaces on the Linux operating system; the music of a prolific and multi-aliased Cornish electronic music artist; support for the LaTeX document preparation system (in which the final version of this thesis will be produced); and the fetishistic worship of vintage IBM mechanical keyboards. The exact content of these communities is irrelevant but is offered as just one tiny example of the wealth of specialized information produced and disseminated by the modern Internet user. But while users continue to possess considerable agency in the production of content, they have little control over online structures which govern how they may produce, use, and share that content.

Photobucket is an image-hosting website that opened in 2004 and allows users who don't have a dedicated server of their own to upload photos which they can then use on blogs, social media, and e-commerce sites. Photobucket offered a

variety of pricing tiers corresponding to different amounts of storage space, including a free (ad-supported) 2GB tier used by many users to host images posted to discussion forums like the ones I visited above. In late June 2017, many people began noticing that product images for third-party sellers on Amazon.com had been replaced by Photobucket images stating, "please update your account to enable third-party hosting."[1] Without any apparent warning, Photobucket had changed its terms of service to prohibit third-party hosting—that is, the posting of images hosted at Photobucket on other websites rather than linking back to a page at Photobucket—at the free pricing tier. A company blog post stated that the previous free ad-supported hosting plan had become unsustainable given the proliferation of ad-blocking software, and explained that users who wished to continue to use Photobucket to host images on other websites would need to subscribe to the paid "Plus 500" plan.[2] At a cost of $39.99 per month or at a discounted yearly rate of $399, the Plus 500 is the most expensive of the three hosting plans that Photobucket offers, with "Plus 50" and "Plus 100" (the numbers correspond to gigabytes of storage) plans offered at annual rates of $59.99 and $99.99, respectively.[3] Inexplicably, the $399 Plus 500 plan is the only one which offers third-party photo hosting, arguably one of the primary features of the

1. Natt Garun, "Photobucket Accused of Blackmail after Quietly Requiring Users to Pay $400 a Year to Hotlink," *The Verge*, July 4, 2017, accessed July 27, 2017, https://www.theverge.com/2017/7/4/15919224/photobucket-broken-images-amazon-ebay-etsy-paid-update.

2. Photobucket Press, "Photobucket Launches Unlimited 3rd Party Hosting Plan," *Photobucket Blog*, July 6, 2017, accessed July 27, 2017, http://blog.photobucket.com/photobucket-launches-unlimited-3rd-party-hosting-plan/.

3. "Photobucket Plus Storage," *Photobucket*, accessed July 27, 2017, http://photobucket.com.

service. Countless users suddenly had their photos in essence held for ransom, and were faced with the difficult decision of either paying a substantial amount of money to re-enable the hosting feature, or spend a substantial amount of time and effort migrating their stored photos away from Photobucket to another hosting solution. Some users even reported being unable to download their stored photos from the service to transfer to a new one until they subscribed to one of the updated plans.[4] Users who decided to stop using Photobucket would have to find a new hosting solution and then update all affected websites where their photos were displayed—a minor nuisance in the case of people using the service to display images in forum conversations or on blogs, but a substantially larger impact on the people using the service as part of an online business.

While there are certainly lessons to be learned from this example on how to go about communicating changes to a widely used service with customers, or the feasibility of arbitrarily pricing products in a way that places customers in a "damned if I pay, damned if I don't" dilemma, the more relevant takeaway from this is that as long as the user is made dependent on the whims of an Internet driven purely by the logic of neoliberal capitalism, they will always be subjected to sudden changes in terms of service which they have no power to negotiate, or prices for services that, though exorbitant, are rationalized as being within what "the market" will bear. While services such as Photobucket have made, for example, the process of sharing images online much more accessible to users of

4. Emma Woollacott, "Amazon Is Looking A Mess - And Photobucket Is To Blame," *Forbes*, last modified July 5, 2017, accessed July 27, 2017, http://www.forbes.com/sites/emmawoollacott/2017/07/05/why-amazon-and-etsy-are-looking-such-a-mess/.

all technical levels than the options available in 1995 (which most likely involved hosting the images to be shared on one's own server or website), the users of 1995 would likely have had far more enduring control over their photos. In this case, the users were penalized because of the failure of an exploitative and unsustainable revenue system to be adequately profitable for Photobucket.

## Conclusions

The Photobucket example perfectly illustrates one of the central concerns of this thesis: with so much power having been either taken from the user or given away in pursuit of the illusion of convenience, the entities which control the structure of the Internet are now the advertising networks seeking continually to increase profits, the software companies fighting against a "piracy" which may or may not exist, and the intelligence agencies attempting to sweep up all user traffic in their bid to eliminate and ultimately predict crime. The user is expected to act in prescribed and predictable ways, and if they fail to contribute towards the goals of these controlling entities, then the Internet can simply be reshaped in a way that more firmly guides the wayward user in their expected roles as consumer, advertising target, or object of surveillance. This is borne out in the examples from the previous case studies: if the user is suspected of illegally sharing the copyrighted software, make the user's access to that software dependent on verification and authorization by the manufacturer. If the user fails to properly participate in the advertising economy by blocking ads or failing to produce a usable profile, then deny the user access to websites, or compromise the tools they

use to achieve these ends. And if the user attempts to violate the most imperative command of the modern Internet—the user shall always be visible—then law enforcement will be forced to assume criminal intent. In none of these cases is the user allowed or encouraged to negotiate these terms; the only way to truly "opt out" is to refuse to use the Internet in the first place.

## Theorizing the User

What is the purpose of attempting to theorize a figure of the Internet user? It's not the sustained study of an Internet culture in an ethnographic mode of inquiry, and neither is it a history of a particular figure or technology. In attempting to define this abstracted figure, I had hoped to try to critically engage with the modern Internet by way of its past. There are numerous narratives describing online life at the time the Internet was new, and in the tradition of the finest late 20th century digital utopianism, they all depict life in this brave new frontier as holding limitless potential for communication and discovery. That Internet no longer exists; as this thesis has made abundantly clear, the onset of commercialization has seen the shape of the Internet change, not to support exploration but to instead guide the users through meticulously arranged tableaux of advertisements and distractions. The user is reduced to a commodity, always working, as Smythe says, "without pay as audience members, marketing consumer goods and services to themselves."[5]

5. Dallas Smythe, "On the Audience Commodity and Its Work," in *Media and Cultural Studies: Keyworks*, ed. Meenakshi Gigi Durham and Douglas M. Kellner, 2nd ed. (Malden, MA: Blackwell Publishing, 2009), 239.

Much early excitement over the Internet revolved around its democratic potential, the promise of decentralized diffusion of knowledge to all who would come to partake of it. This has obviously not come to pass; while the Internet certainly does contain an unimaginable wealth of knowledge, the information is not equally distributed, with limitations placed on geographic location, the value provided by the user as an audience commodity, and the unceasing process of commodification of anything that isn't nailed down—including knowledge itself. Instead, there is the all-seeing electro-panoptic eye, an assemblage of state and commercial surveillance constantly observing the user to ensure their correct and approved use of the Internet.

In working to historicize this abstracted figure, I hope to provide an orienting site from which to launch critiques of a number of related topics: the "origin stories" that represented the early Internet, the steep shift into advertising-driven surveillance capitalism as the animating logic of the Internet, and the role of the individual users themselves in failing to prevent these changes. The ultimate goal of this work in future research is moving towards a radical reconfiguration of the way the Internet itself is theorized, beginning at a rhetorical and discursive level that places the user directly, consciously, and conspicuously at the center of the prevailing logic in order to realize the democratic potential promised in many of the early techno-utopian narratives. This entails developing a new cultural literacy able to identify and critique the

current discourses and practices that have up to now set the user on the periphery.

REFERENCES CITED

Abbate, Janet. *Inventing the Internet*. Cambridge, MA: MIT Press, 2000.

Allen, Matthew. "Web 2.0: An Argument against Convergence." *First Monday* 13, no. 3 (2008). Accessed May 1, 2017. http://firstmonday.org/ojs/index.php/fm/article/view/2139.

Angwin, Julia. "First Library to Support Tor Anonymous Internet Browsing Effort Stops After DHS Email." *ProPublica*. Last modified September 10, 2015. Accessed October 14, 2015. https://www.propublica.org/article/library-support-anonymous-internet-browsing-effort-stops-after-dhs-email.

Angwin, Julia, and Mike Tigas. "How This Company Is Using Zombie Cookies to Track Verizon Customers." *ProPublica*. Last modified January 14, 2015. Accessed July 15, 2017. https://www.propublica.org/article/zombie-cookie-the-tracking-cookie-that-you-cant-kill.

Ankerson, Megan Sapnar. "Writing Web Histories with an Eye on the Analog Past." *New Media & Society* 14, no. 3 (May 1, 2012): 384–400.

Antoviaque, Xavier. "Re: Allowing Acceptable Ads in Adblock Plus." *Adblock Plus*, December 12, 2011. Accessed July 14, 2017. https://adblockplus.org/forum/viewtopic.php?f=1&t=8872&start=30#p53180.

Applebaum, Jacob, Aaron Gibson, J. Goetz, V. Kabisch, L. Kampf, and Leif Ryge. "NSA Targets the Privacy-Conscious." Last modified July 3, 2014. Accessed July 13, 2017. http://daserste.ndr.de/panorama/aktuell/NSA-targets-the-privacy-conscious,nsa230.html.

Asay, Matt. "GPLv3 Hits 50 Percent Adoption." *CNET*. Last modified July 27, 2009. Accessed August 6, 2017. https://www.cnet.com/news/gplv3-hits-50-percent-adoption/.

Associated Press. "Microsoft Campaign Borrows Madonna's 'Ray.'" *Billboard*. Last modified October 16, 2001. Accessed June 30, 2017. http://www.billboard.com/articles/news/78081/microsoft-campaign-borrows-madonnas-ray.

Athow, Desire. "Windows XP End-of-Life: Thanks for All the Fish!" *TechRadar*. Last modified April 6, 2014. Accessed May 7, 2017. http://www.techradar.com/news/software/operating-systems/windows-xp-end-of-life-what-you-need-to-know-1240791.

Ball, James, Bruce Schneier, and Glenn Greenwald. “NSA and GCHQ Target Tor Network That Protects Anonymity of Web Users.” *The Guardian*, October 4, 2013, sec. US news. http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption.

Barbrook, Richard, and Andy Cameron. “The Californian Ideology.” *Science as Culture* 6, no. 1 (January 1, 1996): 44–72.

Barlow, John Perry. “A Declaration of the Independence of Cyberspace.” In *Crypto Anarchy, Cyberstates, and Pirate Utopias*, edited by Peter Ludlow, 27–30. Cambridge, MA: MIT Press, 2001.

Biersdorfer, J. D. “PIRACY AND PRIVACY; Dear User: This Bootleg Copy Will Self-Destruct in 30 Days.” *The New York Times*, September 6, 2001. Accessed November 16, 2016. http://www.nytimes.com/2001/09/06/technology/piracy-and-privacy-dear-user-this-bootleg-copy-will-self-destruct-in-30-days.html.

Blevins, Jeffrey Layne. “Source Diversity after the Telecommunications Act of 1996: Media Oligarchs Begin to Colonize Cyberspace.” *Television & New Media* 3, no. 1 (February 1, 2002): 95–112.

Braden, R., ed. “Requirements for Internet Hosts - Communication Layers.” *Internet Engineering Task Force* RFC1122 (October 1989). Accessed June 4, 2016. http://dx.doi.org/10.17487/RFC1122.

Brügger, Niels. “Website History and the Website as an Object of Study.” *New Media & Society* 11, no. 1–2 (February 1, 2009): 115–132.

Carlton, Danny. “FireFox Is Now Blocked from This and Many of My Other Sites.” *JackLewis.Net*, August 4, 2007. Accessed July 11, 2017. http://jacklewis.net/weblog/archives/2007/08/firefox_is_now.php.

Castells, Manuel. *The Internet Galaxy: Reflections on the Internet, Business, and Society*. Oxford, UK: Oxford University Press, 2002.

Cohen, Noam. “Whiting Out the Ads, but at What Cost?” *The New York Times*, September 3, 2007, sec. Technology. Accessed July 6, 2017. https://www.nytimes.com/2007/09/03/technology/03link.html.

Coleman, E. Gabriella. *Coding Freedom: The Ethics and Aesthetics of Hacking*. Princeton, New Jersey: Princeton University Press, 2012. http://gabriellacoleman.org/Coleman-Coding-Freedom.pdf.

Cormode, Graham, and Balachander Krishnamurthy. “Key Differences between Web 1.0 and Web 2.0.” *First Monday* 13, no. 6 (April 25, 2008). Accessed March 20, 2017. http://dx.doi.org/10.5210/fm.v13i6.2125.

Coursey, David. “Top 10 Things You MUST Know about Win XP.” *ZDNet*. Last modified October 25, 2001. Accessed June 30, 2017. http://www.zdnet.com/article/top-10-things-you-must-know-about-win-xp/.

Cox, Joseph. “This Fake Hitman Site Is the Most Elaborate, Twisted Dark Web Scam Yet.” *Motherboard*. Last modified May 18, 2016. https://motherboard.vice.com/en_us/article/mg77bn/this-fake-hitman-site-is-the-most-elaborate-twisted-dark-web-scam-yet.

DaemonFC. “Re: Allowing Acceptable Ads in Adblock Plus.” *Adblock Plus*, December 12, 2011. Accessed July 14, 2017. https://adblockplus.org/forum/viewtopic.php?f=1&t=8872&sid=f1b1ddfd3237ac059928b22bbd035b82&start=15#p53134.

Dibbell, Julian. *My Tiny Life: Crime and Passion in a Virtual World*. New York, NY: Henry Holt & Company, 1998.

Dingledine, Roger. “Pre-Alpha: Run an Onion Proxy Now!” Last modified September 20, 2002. Accessed July 13, 2017. http://archives.seul.org/or/dev/Sep-2002/msg00019.html.

Dingledine, Roger, Nick Mathewson, and Paul Syverson. “Tor: The Second-Generation Onion Router.” In *Proceedings of the 13th USENIX Security Symposium*, 303–320. San Diego, CA: The USENIX Association, 2004. https://www.usenix.org/conference/13th-usenix-security-symposium/tor-second-generation-onion-router.

Doyle-Burr, Nora. “Despite Law Enforcement Concerns, Lebanon Board Will Reactivate Privacy Network Tor at Kilton Library.” *Valley News*. West Lebanon, NH, September 16, 2015. Accessed October 14, 2015. http://www.vnews.com/home/18620952-95/library-joins-privacy-network.

———. “Emails Describe DHS Tor Concern.” *Valley News*. West Lebanon, NH, September 27, 2015. Accessed October 15, 2015. http://www.vnews.com/news/18760917-95/emails-describe-dhs-tor-concern.

Elkin, Tobi. “Glitzy Times Square Debut for Windows XP.” *Ad Age*, October 25, 2001. Accessed August 4, 2017. http://adage.com/article/digital/glitzy-times-square-debut-windows-xp/33069/.

Evans, David S. “The Online Advertising Industry: Economics, Evolution, and Privacy.” *The Journal of Economic Perspectives* 23, no. 3 (2009): 37–60.

Fairclough, Norman. *Critical Discourse Analysis: The Critical Study of Language*. Language in Social Life. New York, NY: Longman, Publishing, 1995.

———. *Language and Power*. Language in Social Life. New York, NY: Longman, Inc., 1989.

Farivar, Cyrus. “Crypto Activists Announce Vision for Tor Exit Relay in Every Library.” *Ars Technica*. Last modified July 30, 2015. Accessed July 13, 2017. https://arstechnica.com/tech-policy/2015/07/crypto-activists-announce-vision-for-tor-exit-relay-in-every-library/.

———. “Library’s Tor Relay—which Had Been Pulled after Feds Noticed—now Restored.” *Ars Technica*. Last modified September 16, 2015. Accessed July 13, 2017. https://arstechnica.com/tech-policy/2015/09/small-town-library-restores-tor-relay-which-had-gone-dark-for-weeks/.

File, Thom, and Camille Ryan. *Computer and Internet Use in the United States: 2013*. American Community Survey Reports. Washington, DC: U.S. Census Bureau, 2014. Accessed March 19, 2017. https://www.census.gov/content/dam/Census/library/publications/2014/acs/acs-28.pdf.

Fisher, Ken. “Why Ad Blocking Is Devastating to the Sites You Love.” *Ars Technica*, March 6, 2010. Accessed July 6, 2017. https://arstechnica.com/business/news/2010/03/why-ad-blocking-is-devastating-to-the-sites-you-love.ars.

———. “Windows Product Activation: An Early Look.” *Ars Technica*. Last modified February 2, 2001. Accessed November 3, 2016. http://arstechnica.com/information-technology/2001/02/wpa/.

Foucault, Michel. *Discipline & Punish: The Birth of the Prison*. New York, NY: Vintage Books, 1977.

Free Software Foundation. “What Is Free Software?” *GNU Project - Free Software Foundation*. Accessed August 1, 2017. https://www.gnu.org/philosophy/free-sw.html.

Garun, Natt. “Photobucket Accused of Blackmail after Quietly Requiring Users to Pay $400 a Year to Hotlink.” *The Verge*, July 4, 2017. Accessed July 27, 2017. https://www.theverge.com/2017/7/4/15919224/photobucket-broken-images-amazon-ebay-etsy-paid-update.

Gehl, Robert W. “The Archive and the Processor: The Internal Logic of Web 2.0.” *New Media & Society* 13, no. 8 (December 2011): 1228–1244.

———. “The Online ‘Cookie’ Has Turned Stale. Here’s What Advertisers Are Cooking up to Replace It.” *The Week*, February 18, 2014. Accessed July 6, 2017. http://theweek.com/articles/451231/online-cookie-turned-stale-heres-what-advertisers-are-cooking-replace.

Gehl, Robert W., and Casey Boyle. “Cookie Cutters.” *The New Inquiry*, March 20, 2014. Accessed July 6, 2017. https://thenewinquiry.com/cookie-cutters/.

Gilbertson, Scott. “Yahoo, Microsoft Tiff Highlights the Epic Failure of ‘Do Not Track.’” *WIRED*, October 29, 2012. Accessed July 15, 2017. https://www.wired.com/2012/10/yahoo-microsoft-tiff-highlights-the-epic-failure-of-do-not-track/.

Goldschlag, David M., Michael G. Reed, and Paul F. Syverson. “Hiding Routing Information.” In *Information Hiding*, 137–150. Lecture Notes in Computer Science. Cambridge, UK: Springer, 1996. http://dx.doi.org/10.1007/3-540-61996-8_37.

Goldstein, Joseph. “Arrest in U.S. Shuts Down a Black Market for Narcotics.” *The New York Times*, October 2, 2013, sec. N.Y. / Region. https://www.nytimes.com/2013/10/03/nyregion/operator-of-online-market-for-illegal-drugs-is-charged-fbi-says.html.

Gollnick, Clare, and Emily Wilson. *The Truth About the Dark Web: Separating Fact from the Fiction*. White Paper. Terbium Labs, 2016. https://terbiumlabs.com/darkwebstudy.html.

Gomer, Richard, Eduarda Mendes Rodrigues, Natasa Milic-Frayling, and M. C. Schraefel. “Network Analysis of Third Party Tracking: User Exposure to Tracking Cookies Through Search.” In *Proceedings of the 2013 IEEE/WIC/ACM International Joint Conferences on Web Intelligence and Intelligent Agent Technologies*, 1:549–556. Atlanta, GA: IEEE Computer Society, 2013. Accessed July 6, 2017. http://dx.doi.org/10.1109/WI-IAT.2013.77.

Gonzalez, Yanier. “Half of Destructoid’s Readers Block Our Ads. Now What?” *Destructoid*, March 9, 2013. Accessed July 6, 2017.

https://www.destructoid.com/half-of-destructoid-s-readers-block-our-ads-now-what--247904.phtml.

Greenfield, Rebecca. “The Trailblazing, Candy-Colored History Of The Online Banner Ad.” *Fast Company*, October 27, 2014. Accessed July 6, 2017. https://www.fastcompany.com/3037484/the-trailblazing-candy-colored-history-of-the-online-banner-ad.

Haggerty, Kevin D., and Richard V. Ericson. “The Surveillant Assemblage.” *The British Journal of Sociology* 51, no. 4 (December 1, 2000): 605–622.

Hauben, Michael, and Ronda Hauben. “The Social Forces Behind the Development of Usenet.” *First Monday* 3, no. 7 (July 6, 1998). http://firstmonday.org/ojs/index.php/fm/article/view/609.

Hoofnagle, Chris Jay, Ashkan Soltani, Nathan Good, Dietrich James Wambach, and Mika D. Ayenson. “Behavioral Advertising: The Offer You Cannot Refuse.” *Harvard Law & Policy Review* 6, no. 2 (2012): 273–296.

Jonze, Tim. “Aphex Twin Announces New Album SYRO via the Deep Web.” *The Guardian*, August 18, 2014, sec. Music. http://www.theguardian.com/music/2014/aug/18/aphex-twin-announces-new-album-syro-via-the-deep-web.

Kristol, David M., and Lou Montulli. “RFC2109 - HTTP State Management Mechanism.” Internet Engineering Task Force, February 1997. Accessed July 10, 2017. https://tools.ietf.org/html/rfc2109.

Leon, Pedro, Blase Ur, Richard Shay, Yang Wang, Rebecca Balebako, and Lorrie Cranor. “Why Johnny Can’t Opt out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising.” In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 589–598. CHI ’12. New York, NY, USA: ACM, 2012. Accessed July 6, 2017. http://dx.doi.org/10.1145/2207676.2207759.

Lessig, Lawrence. *Code: And Other Laws of Cyberspace, Version 2.0*. New York: Basic Books, 2006.

Lettice, John. “WinXP Beta Testers Still in Open Revolt over Product Activation.” *The Register*. Last modified March 20, 2001. Accessed November 3, 2016. http://www.theregister.co.uk/2001/03/20/winxp_beta_testers_still/.

Levy, Steven. *Hackers: Heroes of the Computer Revolution*. Garden City, NY: Anchor Press/Doubleday, 1984.

Lyon, David. *The Electronic Eye*. Minneapolis, MN: University of Minnesota Press, 1994.

Macrina, Alison, and Nima Fatemi. “Tor Exit Relays in Libraries: A New LFP Project.” *Library Freedom Project*, n.d. https://libraryfreedomproject.org/torexitpilotphase1/.

McDougall, Paul. “Firefox AdBlock Foe Calls For Mozilla Boycott.” *InformationWeek*. Last modified September 12, 2007. Accessed July 6, 2017. http://www.informationweek.com/firefox-adblock-foe-calls-for-mozilla-bo/201805865.

Menegus, Bryan. “The Dark Web Is Mostly Full of Garbage.” *Gizmodo*. Last modified September 21, 2016. Accessed November 8, 2016. http://gizmodo.com/the-deep-web-is-mostly-full-of-garbage-1786857267.

Microsoft Corporation. “About Genuine Windows - Windows Help.” *About Genuine Windows*. Last modified June 14, 2017. Accessed July 3, 2017. https://support.microsoft.com/en-us/help/15087/windows-genuine.

———. “Microsoft Anti-Piracy Solutions Extended to Upcoming Versions of Office, Windows and Visio Products Worldwide.” *News Center*, February 2, 2001. Accessed July 3, 2017. https://news.microsoft.com/2001/02/02/microsoft-anti-piracy-solutions-extended-to-upcoming-versions-of-office-windows-and-visio-products-worldwide/.

———. “Microsoft Piracy - Piracy Basics.” *Protecting Against Software Piracy*. Last modified June 9, 2001. Accessed October 22, 2016. https://web.archive.org/web/20010609221208/http://www.microsoft.com/piracy/basics/xp_activation.asp.

———. “Support for Windows XP Ended.” *Windows XP End of Support*. Last modified April 8, 2014. Accessed May 7, 2017. https://www.microsoft.com/en-us/WindowsForBusiness/end-of-xp-support.

———. “Technical Details on Microsoft Product Activation for Windows XP.” *Microsoft TechNet*. Last modified August 13, 2001. Accessed October 22, 2016. https://technet.microsoft.com/en-us/library/bb457054.aspx.

———. “What Is Windows Product Activation?” *Microsoft - Windows Product Activation Overview*. Last modified 2017. Accessed November 3, 2016. https://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/wpa_overview.mspx?mfr=true.

———. “What Microsoft Is Doing About Piracy.” *Microsoft Protection Against Software Piracy*. Last modified 1998. Accessed July 1, 2017. https://web.archive.org/web/19990429132907/http://microsoft.com:80/piracy/microsoft/default.htm.

Miles, Stephanie. “Microsoft Consolidates Windows Development Efforts.” *CNET News*, January 24, 2000. Accessed August 4, 2017. https://web.archive.org/web/20121107235539/http://news.cnet.com/Microsoft-consolidates-Windows-development-efforts/2100-1040_3-236021.html.

Mook, Nate. “The Truth About Windows Activation.” *BetaNews*. Last modified May 18, 2001. Accessed May 7, 2017. https://betanews.com/2001/05/18/the-truth-about-windows-activation/.

National Security Agency. “Tor Stinks.” *Electronic Frontier Foundation*. Last modified October 4, 2013. https://www.eff.org/document/2013-10-04-guard-tor-stinks.

Oberoi, Ankit. “The History of Online Advertising.” *AdPushup Blog*, July 3, 2013. Accessed July 10, 2017. https://www.adpushup.com/blog/the-history-of-online-advertising/.

O’Reilly, Tim. “Design Patterns and Business Models for the Next Generation of Software.” *O’Reilly Media*. Last modified September 30, 2005. Accessed May 2, 2017. http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html.

Palant, Wladimir. “Allowing Acceptable Ads in Adblock Plus.” *Adblock Plus and (a Little) More*, December 5, 2011. Accessed July 6, 2017. https://adblockplus.org/development-builds/allowing-acceptable-ads-in-adblock-plus.

———. “An Approach to Fair Ad Blocking.” *Adblock Plus and (a Little) More*, May 11, 2009. Accessed July 11, 2017. https://adblockplus.org/blog/an-approach-to-fair-ad-blocking.

———. “Re: Allowing Acceptable Ads in Adblock Plus.” *Adblock Plus*, December 5, 2011. Accessed July 14, 2017. https://adblockplus.org/forum/viewtopic.php?p=52838#p52838.

Photobucket Press. “Photobucket Launches Unlimited 3rd Party Hosting Plan.” *Photobucket Blog*, July 6, 2017. Accessed July 27, 2017. http://blog.photobucket.com/photobucket-launches-unlimited-3rd-party-hosting-plan/.

Rao, Leena. “Yahoo Quietly Pulls The Plug On Geocities.” *TechCrunch*, April 23, 2009. Accessed June 28, 2017. http://social.techcrunch.com/2009/04/23/yahoo-quietly-pulls-the-plug-on-geocities/.

RedneckBabe. “Re: Allowing Acceptable Ads in Adblock Plus.” *Adblock Plus*, December 12, 2011. Accessed July 14, 2017. https://adblockplus.org/forum/viewtopic.php?f=1&t=8872&start=30#p53199.

Reed, Michael G., Paul F. Syverson, and David M. Goldschlag. “Anonymous Connections and Onion Routing.” *IEEE Journal on Selected Areas in Communications* 16, no. 4 (May 1998): 482–494.

Rheingold, Howard. *The Virtual Community: Homesteading on the Electronic Frontier*. Cambridge, MA: MIT Press, 2000.

Sarikakis, Katharine. “Ideology and Policy: Notes on the Shaping of the Internet.” *First Monday* 9, no. 8 (August 2, 2004). Accessed April 12, 2017. http://dx.doi.org/10.5210/fm.v9i8.1167.

Schofield, Jack. “Ad Blocking Is Theft, so Block Firefox Instead (Updated).” *The Guardian*, August 19, 2007, sec. Technology. Accessed July 6, 2017. https://www.theguardian.com/technology/blog/2007/aug/19/adblockingis.

Scholz, Trebor. “Market Ideology and the Myths of Web 2.0.” *First Monday* 13, no. 3 (March 3, 2008). Accessed March 20, 2017. http://dx.doi.org/10.5210/fm.v13i3.2138.

Scott, John. *A Matter of Record: Documentary Sources in Social Research*. Cambridge, UK: Polity Press, 1990.

Selvin, Joel. “Q and A With Brian Eno.” *SFGate*. Last modified June 2, 1996. Accessed June 30, 2017. http://www.sfgate.com/music/popquiz/article/Q-and-A-With-Brian-Eno-2979740.php.

Singel, Ryan. “Oct. 27, 1994: Web Gives Birth to Banner Ads.” *WIRED*, October 27, 2010. Accessed July 8, 2017. https://www.wired.com/2010/10/1027hotwired-banner-ads/.

Smith, Will. “The 10 Most Important Things You Must Know About Windows XP.” *Maximum PC*, October 2001.

Smythe, Dallas. “On the Audience Commodity and Its Work.” In *Media and Cultural Studies: Keyworks*, edited by Meenakshi Gigi Durham and Douglas M. Kellner, 230–255. 2nd ed. Malden, MA: Blackwell Publishing, 2009.

Solomon, Kate. “Windows 7 Use Finally Overtakes Windows XP.” *TechRadar*. Last modified October 17, 2011. Accessed May 7, 2017. http://www.techradar.com/news/computing/pc/windows-7-use-finally-overtakes-windows-xp-1034482.

Spanbauer, Scott. “Latest Windows XP Beta Adds Strict Copy Protection.” *PC World.Com* (March 25, 2001). Accessed November 16, 2016. http://search.proquest.com/docview/200751519/abstract/C2FC31DD6A944DCFPQ/1.

St. Louis, Christopher. “For Your Protection: State Surveillance and Narratives of Risk in Contemporary Japan.” Master’s Thesis, University of Tokyo, 2014.

Staff. “Editorial: Privacy Concerns and the Kilton Library.” *Valley News*. West Lebanon, NH, September 15, 2015, sec. Opinion. Accessed July 21, 2017. http://mobile.vnews.com/Archives/2015/09/edit-tor-vn-091515.

Stallman, Richard. “Meme 2.04.” Interview by David S. Bennahum. Electronic newsletter, 1996. Accessed July 30, 2017. http://memex.org/meme2-04.html.

Stallman, Richard M. *Free Software, Free Society: Selected Essays of Richard M. Stallman*. Edited by Joshua Gay. 2nd ed. Boston, MA: Free Software Foundation, 2010.

———. “The GNU Manifesto.” *GNU Project - Free Software Foundation*. Last modified 1985. Accessed August 1, 2017. https://www.gnu.org/gnu/manifesto.html.

———. “The GNU Operating System and the Free Software Movement.” In *Open Sources: Voices from the Open Source Revolution*, edited by Chris DiBona, Sam Ockman, and Mark Stone, 31–38. Sebastopol, CA: O’Reilly Media, Inc., 1999.

Syverson, Paul. “Our Sponsors.” *Onion Routing*. Last modified 2005. Accessed July 20, 2017. https://www.onion-router.net/Sponsors.html.

Templeton, Brad. “Reaction to the DEC Spam of 1978.” Accessed July 8, 2017. http://www.templetons.com/brad/spamreact.html.

Terranova, Tiziana. *Network Culture: Politics for the Information Age*. London: Pluto Press, 2004.

Tigas, Mike. “A More Secure and Anonymous ProPublica Using Tor Hidden Services.” *ProPublica*. Last modified January 13, 2016. https://www.propublica.org/nerds/item/a-more-secure-and-anonymous-propublica-using-tor-hidden-services.

Weiser, Benjamin, and Doreen Carvajal. “International Raids Target Sites Selling Contraband on the ‘Dark Web.’” *The New York Times*, November 7, 2014, sec. Europe. https://www.nytimes.com/2014/11/08/world/europe/dark-market-websites-operation-onymous.html.

Wilcox, Joe. “Microsoft Readies XP for Late October.” *CNET News.Com*. Last modified May 9, 2001. Accessed June 30, 2017. https://web.archive.org/web/20011130011654/http://news.cnet.com/news/0-1003-200-5870654.html.

———. “Windows XP Marketing Tab to Hit $1 Billion.” *CNET*. Last modified June 26, 2001. Accessed June 30, 2017. https://web.archive.org/web/20140201144711/http://news.cnet.com/2100-1001-269032.html.

Williams, Sam. *Free as in Freedom: Richard Stallman’s Crusade for Free Software*. Sebastopol, CA: O’Reilly Media, Inc., 2002.

Wilson, Dave. “Safeguards Punish Consumers, Not Pirates.” *Los Angeles Times*, October 25, 2001. Accessed November 3, 2016. http://articles.latimes.com/2001/oct/25/news/tt-61351.

Winner, Langdon. “Do Artifacts Have Politics?” *Daedalus* 109, no. 1 (1980): 121–136.

Woollacott, Emma. “Amazon Is Looking A Mess - And Photobucket Is To Blame.” *Forbes*. Last modified July 5, 2017. Accessed July 27, 2017. http://www.forbes.com/sites/emmawoollacott/2017/07/05/why-amazon-and-etsy-are-looking-such-a-mess/.

Zittrain, Jonathan. *The Future of the Internet--And How to Stop It*. New Haven, CT: Yale University Press, 2008.

Zuboff, Shoshana. “Big Other: Surveillance Capitalism and the Prospects of an Information Civilization.” *Journal of Information Technology* 30, no. 1 (2015): 75–89.

Zuckerman, Ethan. “The Internet’s Original Sin.” *The Atlantic*, August 14, 2014. Accessed July 6, 2017. https://www.theatlantic.com/technology/archive/2014/08/advertising-is-the-internets-original-sin/376041/.

"About Adblock Plus." Last modified November 19, 2010. Accessed August 9, 2017. https://web.archive.org/web/20101119073306/https://adblockplus.org/en/about.

"Allowing Acceptable Ads in Adblock Plus." *Adblock Plus*. Accessed July 14, 2017. https://adblockplus.org/acceptable-ads.

"GeoCities Special Collection 2009." *Internet Archive*. Accessed June 28, 2017. https://archive.org/web/geocities.php.

"Google Launches Self-Service Advertising Program." *News from Google*. Last modified October 23, 2000. Accessed July 10, 2017. https://web.archive.org/web/20120313164802/http://www.google.com/press/pressrel/pressrelease39.html.

"Internet Archive: Wayback Machine." Accessed June 29, 2017. https://archive.org/web/.

"Windows XP Service Pack 2: What's New for Internet Explorer and Outlook Express." *Microsoft.Com*. Last modified August 4, 2004. Accessed July 6, 2017. https://web.archive.org/web/20051212084214/http://www.microsoft.com:80/windowsxp/sp2/ieoeoverview.mspx.