"It Doesn't Have to Be This Way": Hacker Perspectives on Privacy

Kevin Steinmetz & Jurg Gerber*

> We face a lot of troubling times ahead with regards to surveillance. Most of the power, for the moment at least, remains in our hands and in our minds, should we choose to use them. It is our acceptance of the elements of a surveillance state which will give it the most strength and solidify its presence for future generations. It doesn't have to be this way.
> —Emmanuel Goldstein, "The Whole World's Watching" (2008, 5)

If a person were to only consult news media, he or she would gain the impression that the world is constantly under threat of computer hackers eroding our technological infrastructure, national security, and—perhaps most immediately frightening to many—our personal privacy. Much attention has been directed toward hackers recently, in light of the numerous controversies surrounding the escapades of hacker groups like Anonymous and the disbanded Lulz Security/LulzSec (Olson 2012); concerns over consumer financial security, as demonstrated in the occasion of the recent breach of credit card data at Target (Newman 2013); and a plethora of other hacking occurrences.[1] Perhaps now more than ever, hackers are perceived as a tremendous threat, particularly to personal privacy.

Scholars have spent a great deal of time examining public perceptions towards hackers (Halbert 1997; Holt 2009; Skibell 2002; Thomas 2005). Hacking, however, is often shrouded in a veil of social construction, perhaps as a result of the fact that the public has "little direct contact with computer hackers," which makes their image "particularly susceptible to shifts in public perception" (Skibel 2002, 343; Hollinger 1991; Taylor 1999). In what has been termed the "golden age" of hacking, hackers were often perceived as "ardent (if quirky) programmers, capable of brilliant, unorthodox feats of machine manipulation… [whose] dedica-

* **Kevin F. Steinmetz** (email: kfsteinmetz@ksu.edu) is an assistant professor in the Department of Sociology, Anthropology, and Social Work at Kansas State University. **Jurg Gerber** (email: icc_jxg@shsu.edu) is a professor in the Department of Criminal Justice and Criminology at Sam Houston State University. The authors would like to thank the Graduate Standards and Admissions Committee for the fellowship opportunity that permitted this research to take place. In addition, gratitude must be extended to the reviewers who examined this manuscript, particularly Reviewer #2 whose comments were particularly helpful and incisive.

tion bordered on fanaticism and [whose] living habits bordered on the unsavory" (Nissenbaum 2004, 196). Currently, hackers are often portrayed as "young men whose pathological addiction to the internet leads to elaborate deceptions, obsessive quests for knowledge, and bold tournaments of sinister computer break-ins" (Coleman and Golub 2008, 256). Although the term encompasses a much broader community than just those who commit network intrusions, almost any time a computer-related crime is committed, the media refer to the violator as a hacker (Holt 2009; Turgeman-Goldschmidt 2011). Thus, hackers have been constructed as some sort of digital malcontents capable of causing computerized chaos, including imposing on network privacy.

Though certainly no one can argue that at least some hackers pose a threat to privacy, few seem to consider how hackers themselves view privacy and related issues. Hackers are often at the nexus of technology, politics, and control. Surveillance measures have proliferated in what has been referred to as a culture of control (Garland 2002), and demands for security through monitoring encroach on personal privacy—as most controversially demonstrated by recent events concerning the National Security Agency and their PRISM program. Examining hackers' perceptions of privacy may prove fruitful for future studies of hacker culture and behavior, because hackers are: (a) tremendously affected by increases in modern surveillance assemblages, which often encroach on domains hackers work in (computers, the Internet, etc.); (b) scrutinized heavily by media, government, and the public (Hollinger 1991; Skibell 2002; Turgeman-Goldschmidt 2011); and (c) often curious and interested in exploration (thus presenting a potential privacy threat to others) while also being vehement advocates of privacy themselves.

As a step toward understanding these perceptions, the current study engages in a qualitative content analysis of *2600: The Hacker Quarterly*. The magazine was created by Emmanuel Goldstein (pseudonym of Eric Corley, who adopted his name from the supposed enemy of the state in Orwell's *1984*) and began publication in 1984. *2600* is a hacker zine acknowledged to be one of the "first significant hacker publications" (Thomas 2005, 604), and it features articles written by members of the hacking community for hackers.[2] Before discussing the results of the analysis, a brief overview of the scholarly literature on hacking is provided as well as a discussion of the data gathering process and qualitative analysis approach. The results are presented focusing primarily on 10 themes that emerged in the analysis and are discussed in the context of technolibertarianism and crypto-anarchy.

Literature Review

The term "hacking," as related to computers and technology, has been around since the late 1950s or early 1960s (Levy 1984). Many perspectives and approaches have been adopted to examine this phenomenon in the academic literature. Scholars have studied hackers' cultural practices and shared meanings as well as the formation of hacker identities (Coleman 2010, 2012, 2013; Hollinger 1991; Holt 2009, 2010a,

2010b; Turgeman-Goldschmidt 2005, 2011; Warnick 2004). The social construction of hacking has also been analyzed, specifically focusing on how the image of the hacker has changed over time (Halbert 1997; Skibell 2002; Thomas 2005). Hacktivism, a portmanteau of "hacking" and "activism," has also been examined by scholars as a phenomenon heavily related to hacking culture (Jordan and Taylor 2004; McKenzie 1999; Meikle 2002; Taylor 2005; Van Laer and Van Aelst 2010), and some researchers have investigated the hackers' demographic and psychological characteristics (Bachman 2010; Schell 2010; Schell and Holt 2010).

Perhaps more relevant for criminology, some research focuses on the creation of viruses and malware, computer intrusions, website defacements, and identity theft (Furnell 2010; Higgins 2010; Jordan and Taylor 1998; Nichols et al. 2000; Woo et al. 2004). Criminological theory testing has been conducted concerning hacking (Bossler and Burruss 2010; Morris 2010), and previous research has also examined hackers' perceptions of government, law, and law enforcement (Steinmetz and Gerber 2014).

In 1984, Levy introduced a concept that is perhaps most relevant to understanding hacker perspectives on surveillance and privacy: the hacker ethic. At the time, this ethic involved the idea that "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!" (Levy 1984, 40). The hacker ethic can be viewed as a particular ontological perspective adopted by members of the hacking subculture. Both a philosophy of liberalism (Coleman and Golub 2008) and a belief that the world operates as a system or a series of interoperating systems (Warnick 2004) underpin this viewpoint. This perspective gives rise to multiple features of the hacking subculture. First is the belief that information wants to be free (Levy 1984; Stallman 2002). As Stallman (2002, 43) specifies, this is not "free" in the sense of "free beer," but free as in "free speech." And since information wants to be free, restrictions on access to information are perceived as abhorrent (Hollinger 1991; Levy 1984; Stallman 2002), which helps to explain many efforts hackers have been known to make in circumventing technological security measures (Hollinger 1991).

A second feature of the hacker ethic involves what Levy (1984) has described as the hands-on imperative—a desire to be engaged in an active, hands-on manner. From a Weberian perspective, this imperative has been described as a move beyond the protestant ethic and toward a blurring of labor and leisure that requires an active, rather than passive, approach to the consumption of technology and media (Brown 2008; Himanen 2001). In this sense, hackers dedicate themselves to learning about and tinkering with systems, which often leads to (a) the creation of new or improved systems and (b) the ability to manipulate them. This do-it-yourself mentality of exploration and manipulation even extends beyond the technological to the social realm, involving a practice referred to as social engineering (Coleman and Golub 2008; Mitnick and Simon 2002, 2011; Thompson 2006). This feature

of the hacker ethic has also lead to the development of the free and open-source software movement (F/OSS), involving the collaborative creation of freely and openly available programs, applications, and operating systems (Coleman and Golub 2008; Dafermos and Söderberg 2009).

Technological utopianism comprises the final feature of the hacker ethic (Barbrook and Cameron 2001). Here, technology is viewed as a potential remedy to many social problems. Any shortcomings experienced in any domain of life are thought to have a potential technological solution. The consequence is a desire to use technology to circumvent restrictions (often meant to obstruct access to systems) and to protect oneself, particularly regarding privacy (Coleman and Golub 2008).

In sum, the hacker ethic combines a liberal philosophy and a systemic ontology to engender (a) a belief that information wants to be free, (b) a desire to be hands-on with systems of all sorts, and (c) a sense of technological utopianism. Although Coleman (2012) convincingly argues that the hacking subculture is so diverse that one ethic may not serve to adequately capture the entirety of its internal dynamics, the aforementioned features converge in a body of political thought, shared within high-technology cultural circles, that can be useful for understanding hacker perspectives on privacy: technolibertarianism and, relatedly, crypto-anarchy. As described by Taylor and Jordan (2004, 134):

> The term technolibertarian refers to those closely involved within the computer industry who espouse strong libertarian and free-market political principles and closely associate them with the promotion of the e-economy. Their views frequently articulate a preference for a society as free as possible from regulation, social ties and, generally, the obligations that inevitably stem from community relations in the real world.

Such a perspective is a manifestation of the liberalism that permeates tech culture, including the hacker community (Coleman and Golub 2008). One extension of this philosophy is crypto-anarchy, which arose from the public key cryptography movement (Levy 2001). Situated in the context of technolibertarianism and technological utopianism, crypto-anarchy holds the belief that cryptography is a key solution to protecting privacy, particularly against intrusions by the state (Frissell 2001; May 2001; Hughes 2001). As discussed below, these bodies of thought are key to understanding hacker perspectives on privacy.

Method

This study involves a content analysis of the US-based magazine *2600: The Hacker Quarterly* (referred to hereafter as *2600*). *2600* features full-length articles in addition to editorials, letters to the editor, short stories, and book reviews. The zine currently enjoys wide circulation, which includes the shelves of a major bookseller such as Barnes & Noble. Due to its popularity, historical significance, hacker-

authored content, and its role as a forum to discuss political perspectives within the hacking community, *2600* is an ideal publication for analysis. The current study focuses in particular on the perceptions of privacy expressed by the authors in their writings for the journal.[3]

Sample

The sample for this study was drawn from 41 issues of *2600*. The chosen time frame begins with the Spring 2002 volume because this issue followed shortly after the events of 9/11—an event that triggered a massive shift in security and surveillance policy in the United States (Cole and Lobel 2007). Hackers were (and continue to be) greatly affected by the developments in the area of cybersecurity and the increases in scrutiny that have followed the beginning of the War on Terror. The sample includes all issues from Spring 2002 up to Spring 2012—the most recent issue at the time of data gathering and analysis. As a result, the sample includes just over 10 years of publications. The particular units of analysis within these issues include articles, editorials, book reviews, and short stories; in total, over 839 articles, 41 editorials, 8 short stories, and 2 reviews (collectively referred to as items) written by 611 different authors were examined for any mention of privacy, surveillance, or related security issues (see Table 1). Any such mention was flagged and logged in an electronic dataset, together with a note briefly describing the content of the item and providing context for later analysis. This process created a subsample for analysis that consisted of 188 articles, 27 editorials, and 2 short stories written by 161 different authors—a total of 24.3 percent of the full sample.

Table 1: Descriptive Statistics

	Full sample	Subsample
Total # of articles	893	217
Articles	839	188
Editorials	41	27
Reviews	2	0
Short stories	8	2
Total # of authors	611*	161

* Some duplicates were included for authors reporting similar names, such as kaige and kaigeX. Omitting duplicates brings the number down to 608.

Coding Procedure

To code and analyze the data, this study employs a grounded theory–based analytical approach (Charmaz 2006; Strauss and Corbin 1998). Grounded theory methods of analysis "consist of flexible strategies for focusing and expediting qualitative

data collection" and "provide a set of inductive steps that successively lead the researcher from studying concrete realities to rendering a conceptual understanding of them" (Charmaz 2002, 675). Accordingly, the coding procedure used in the current study included three stages of analysis. In the first stage, each passage extracted from the items in *2600* was given a short description of how the author presented the privacy or surveillance issue. At this stage, the objective was to describe as plainly as possible what the author was conveying about these issues. The second stage of analysis involved examining each passage again alongside the results of the first stage. Here, passages and descriptions were distilled down into shorter descriptions that attempted to capture the essence of the author's argument. The third stage involved comparing the results of the first two waves to generate common themes. The remainder of this article focuses on the overarching themes that emerged during the analysis.

Results

Major Themes

Like many discussions of privacy and surveillance, the perspectives presented here involve a number of twists and turns. Indeed, numerous themes emerged from the analysis—so many that it would be difficult to discuss each of them in detail. For this reason, we will only focus here on a limited number of topics, divided into two sections: major and minor themes. Major themes were more prevalent in the data and will be afforded more time in the discussion; minor themes were less prevalent and will thus be given proportionately less attention. The four major themes discussed in this section are: dualisms, responsibility to protect privacy, ubiquity of threats to privacy, and the role hackers play in protecting privacy. Table 2 shows the frequency of each of these themes in the data.

Table 2: Major Themes

Themes	Total (% of articles in subsample)
Dualisms	168 (77.42%)
Responsibility	111 (51.15%)
Ubiquity	52 (23.96%)
Role Hackers Play	47 (21.66%)

Dualisms

The most prevalent theme within the data is the notion that various actors and institutions can be both protectors and threats to privacy (n = 168; 77.42 percent).

Such dualism is discussed with particular reference to: (a) the government and its various institutions, agencies, and actions; (b) business; and (c) technology. Hackers also discussed individuals dualistically—i.e., people are seen simultaneously as agents to protect their own privacy and as tremendous threats to themselves. For purposes of organization, this dualism is acknowledged here but discussed in greater detail in the following section on responsibility.

The first dualism explored here is the one that sees government as both a threat to privacy and a (potential) protector of it. Very few domains of governmental action were left untouched by the authors. For instance, law enforcement was implicated as having a dualistic potential. OSIN (2007, 6) states: "One of the most used weapons of today's organized crime syndicate is the secret warrantless search… Surely such evil doesn't exist in the Land of the Free and Home of the Brave!" Legislation is also implicated as a threat, which author area_51 (2002, 54) describes with regard to the Consumer Broadband and Digital Television Promotion Act—a bill that did not pass but is described here as a huge potential threat to privacy:

> Big Brother now wants to have the capability to "put a cop in every computer." In the "Consumer Broadband and Digital Television Promotion Act" (S 2048 IS), Senator Hollings (D) of South Carolina has proposed a bill that would force the computer and consumer electronics industry to place a copy-protection mechanism in a device which "reproduces, displays or retrieves or accesses any kind of copyrighted work." This definition would allow for all computers, MP3 players, TV sets, cable boxes, VCRs, DVD players, digital cameras, stereo systems, CD-Burners, and scanners, not to mention a host of other devices, to be subject to the regulation of the government.

Other sources of threats to privacy posed by the government include policies like the War on Terror and War on Drugs, increasing surveillance, the centralization and retention of data, and collaboration (cooperatively or coercively) with businesses to access personal information. If it is perhaps unsurprising to find that hackers believe that government poses a threat to personal privacy in various capacities, discussions of the various ways in which the government can act to protect privacy may appear less predictable. Authors Malf0rm3dx and Megalos (2011, 30), for example, discuss legislation meant to protect privacy—even if it may not be as effective as they wish:

> And let's not forget the Electronic Communications Privacy Act, 18 USC 2510, that prohibits anyone from intercepting messages sent to display pagers both numeric and or alphanumeric. And, while these laws are in place, there is absolutely no technological means that is stopping a person

> from accidentally or intentionally intercepting these transmissions and using them for personal gain.

Litigation or lawsuits are also discussed as potential protectors of privacy, here as a means of redress against the actions of Google:

> Due to malice (unlikely), or just plain screwing up (much more likely, in my opinion), Google has also been collecting actual network data, not just management packets which describe the network. Why they might have done this remains a mystery – one which many, many governmental and civil lawsuits are likely going to be trying to answer. (Dragorn 2010, 53)

In some capacity or another, through law enforcement, litigation, or various policies and actions, the government is portrayed as being capable of both breaking privacy and upholding it—a finding that contradicts some stereotypes of hackers as firmly anti-authoritarian.

Business was also presented in a dualistic fashion by the authors of *2600*. Businesses are often said to threaten privacy through the collection of data for marketing purposes and the subsequent selling of said data. Bland Inquisitor (2002a, 11) also describes business as threatening privacy by corrupting legislation:

> In 1991, a bill called the Telephone Consumer Protection Act (TCPA) was passed. This act was supposed to keep you safe and free of unwanted calls, but by the time the corporations had their say, very little of this bill remained to protect us. The upside is that there are still a few bits of useful information hidden in the jargon and some of the protective devices made it through.

Conversely, the authors also describe business as capable of protecting privacy—primarily through the creation and upholding of policies that refuse to disseminate the private information of customers/users. At the very least, hackers expect businesses to be capable of protecting privacy, even if they seldom live up to this expectation. Although b0rn_slippy (2006, 7) ultimately finds Facebook to be lacking in security at the time of writing, he at least acknowledges that the company makes efforts to protect user information (or at least claims to): "In comparison to MySpace, recently affected by Samy's famous worm, Facebook makes widely publicized claims to high security and privacy."

Perhaps most interestingly, given that hackers have often been described as cyber-utopians (Barbrook and Cameron 2001), in the writings analyzed here technology was described not only as a means to guard one's private information, but also as a potential major threat to privacy. Editor Goldstein (2009, 4) discusses the threat technology (and to some extent, the convenience it affords) poses to privacy:

> Our entire worlds go into our phones and all of our contacts have corresponding files with as much detail as we care to store about them. Yes, you can have not only a picture and name pop up when someone calls you, but their most recent post on a social networking site so you can gauge their mood or know what they've been up to before you even start talking to them. You can have little essays written about everyone you know and every bit of information you have on them, all at your fingertips anytime. Big Brother has nothing on *this* level of surveillance.

At the same time, however, technology is also discussed as a solution to privacy problems. Author p4nt05 (2010, 46) describes the use of the technological measure called "darknets" to protect privacy over the Internet: "The term darknet can mean many things: within the context of this article we discuss it as 'a set of softwares and systems that are private but Internet accessible, usually used by a group of friends or associates for privacy.'"

Responsibility

Another theme that permeated hackers' discussions of privacy and surveillance was the idea of responsibility (n = 111; 51.15 percent). This theme seemed to hinge on the idea that those who have possession or control of some information are also those who are responsible for protecting that information. Therefore, individuals are responsible for protecting their own privacy. For example, Lifeguard (2011, 16) describes his vigilance to protect his privacy: "That Christmas, I got a modem and started calling BBSes. Shared knowledge amplified intelligence. I also learned to be cautious and think about what sort of 'trail' I might be leaving with my activities." Consequently, users are seen as putting their own privacy at risk through irresponsibility. With regard to recent widespread concerns about the threat social networks pose to privacy, Dragorn (2007, 52) asserts that in these settings, users are the ones who are actually responsible for any breaches in privacy, since they are the ones who select what to share and upload: "Social networks have often been considered a major privacy risk, but the risks are directly tied to the information that the user is willing to share."

Part of one's personal responsibility for privacy involves a duty to act when privacy is jeopardized. Author docburton (2002, 43) advocates for resistance through civil disobedience against a company whose technology invades individuals' privacy:

> Well, I hope this gave you an overview of what online ad companies do and how they do it. It's up to us to explore their structure more (there is plenty of leaked info around) and point out to them the weaknesses in their system. Maybe throw a little civil disobedience in there too to let them know that you are not a person who is willingly exploited so that some huge company can sell you crap that you don't need. Good luck!

In the end, individuals are in control of their personal information, and as such they need to be mindful of threats and take actions against them—through activism, resistance, or personal measures.

When personal information leaves the individual, however, whoever owns the system in which the data is collected is charged with the responsibility of protecting those data. Criticizing Bank of America, malpelo93 (2008, 53) states, "It would seem that Bank of America does not care about the privacy and security of their customers' credit card statements enough to fix this critical flaw in their website." Acrobatic (2012, 49) discusses how these companies should be more responsible with the personal data they hold:

> In December of 2011, members of activist group Anonymous released a slew (over 860,000 records) of private data stolen from think-tank Stratfor. While I don't condone the theft, I do 1) condone the attention it brings to a firm that prides itself on being both intelligent and secure as a means of showing the public that no data is entirely secure and, 2) as a means of pointing out these insecurities in the hopes that it will make them more intelligent and more secure with our data.

In this manner, whoever has access to personal information is considered responsible for its protection. The responsibility to protect private data is transferable.

Ubiquity

Another theme that emerged from the data is an overall perception that threats to privacy are ubiquitous (n = 52; 23.96 percent). The precise nature of this ubiquity, however, varies. Eberhard (2008, 26) discusses the spread of the surveillance state in the United States following the events of 9/11:

> Meanwhile we are busily transforming the Land of the Free into a High Tech Surveillance Society of our own. In the name of preventing terrorism in this post-9/11 world, we have come to accept the Patriot Act, video cameras watching us along highways and intersections, more video cameras in other public places, invasive airport screening, scrutinized financial transactions, widespread wiretaps, surveillance of our online activities, efforts to create national identity cards, face recognition equipment at sporting events and lots more.

In addition, the prevalence of surveillance and other threats is said to have increased over the years:

> Unlike in the world of fiction, when change occurs, it doesn't happen overnight. It's a very gradual process that takes place one step at a time. But if you look back and take in all of the changes that have occurred in

> a particular number of years, you will be shocked at how much our way of life has changed. Think of technology as parallel to this. How different is the world of today with regard to telephones and computers than, say, the world of 20 years ago? Apply that to the surveillance, fear, and surrendering of rights that have been ongoing in that same time period and it's downright scary. (Goldstein 2006, 5)

Contributing to this ubiquity of threats is the rise in data retention by both governmental and business organizations as well as the centralization of databases filled with personal information. The Prophet (2002, 24) describes the proliferation of database centralization:

> To help it fight the insane "war on [some] drugs," the federal government has already connected the databases of the Customs Services, the Drug Enforcement Agency, the IRS, the Federal Reserve, and the State Department.... Additionally, the United States has relatively few data protection laws (particularly concerning the collection of data for commercial purposes), meaning the extensive use of computer matching has led to a "virtual" national data bank. With only a few computer searches, and without obtaining a search warrant, law enforcement can gather a comprehensive file on virtually any US citizen in a matter of minutes.

According to hackers, therefore, threats to privacy are rife in our society and have been growing over time. The increasing trend of data retention and centralization contributes to this threat. Apparently, the more connected individuals become, the more connected organizations become as well.

The Role Hackers Play

The last major theme that emerged from the data concerns the role that hackers claim to have regarding the protection of privacy (n = 47; 21.66 percent). Indeed, rather than simply enumerate existing problems with privacy, the authors believe that hackers and the greater hacker community can play a role in solving them. The first role involves exploring systems (social and technical) to find vulnerabilities. One example concerns an alleged privacy vulnerability in ASUS's repairs system:

> In response to this major security hole, as well as breaches of data privacy statutes, I sent an anonymous letter to ASUS making them aware of their situation and recommending a two-credential authentication change as a solution to the problem. It is a shame that I had to write them anonymously… We must hide our creative and specialized work for fear of repercussion, while in the end (and beginning) we are only helping. (bTrack3r2003 2011, 25)

This example leads into the next role the authors discuss: educating others about the privacy risks around them.

> We must continue to educate our fellow humans about open source software, loss of privacy, information security, the tyranny of tiered Internet services, and the power that every individual has access to. If we don't, we may wake up on day to find that we do not have Internet freedom any more. (Brown 2008, 11)

Other roles include resisting attempts to encroach on privacy as well as, more generally, focusing on, caring about, and protecting privacy. Overall, the authors of *2600* seem to insist that hackers do not, and should not, have a passive role in personal and societal privacy problems. Their role seems to be primarily oriented toward finding vulnerabilities and other threats to privacy and educating others—which, as bTrack3r2003 (2011/2012) points out, is not always appreciated as hackers often have a bad reputation in society.

Minor Themes

As previously stated, a number of minor themes emerged from the data, though with a relatively lower prevalence (see Table 3). The first involves a differentiation between the rights to privacy of common individuals and of those in power. In short, the author seem to believe that the more power a person possesses, the lower their entitlement to privacy. This was primarily articulated through an insistence that although secret surveillance is undesirable, the erosion of secret-keeping by those in positions of authority is desirable (n = 29; 13.36 percent). In decrying the NSA's secrecy, for example, one author stated: "The NSA has also (presumably) been granted secret powers to do secret things in secret facilities constructed at tandem across the US, but whether or not they have been granted this authority is in itself a secret" (The Prophet 2009, 13). In short, those in authority should not be allowed to hold privacy—a value dearly held at the individual level—because of the potential for its abuse.

Table 3: Minor Themes

Themes	Total (% of articles in subsample)
Privacy of individuals vs. authorities	29 (13.36%)
Hackers' exemption	28 (12.90%)
Collateral damage	23 (10.60%)
Privacy linked to freedoms/liberties	11 (5.07%)
Hackers as scapegoats	10 (4.61%)

A second minor theme involves a seeming contradiction in some of the authors' beliefs. In essence, it seems that violations of privacy are generally decried except when these violations are perpetrated by hackers. A number of reasons are given for why hackers could violate privacy, including curiosity, exploration, and to find vulnerabilities. As Xyzzy (2007, 19) states, describing the claimed curious nature of hacking:

> Like most people I don't go looking for trouble. I've never made a hobby of trying to steal passwords or violate people's privacy. But when an opportunity slaps you right in the face, I'm as curious as the next person.

In short, it seems that privacy is to be held as sacred but hackers are exempt from this by-and-large. Of course, this exception may come with some qualifications, for example: "Do not invade the privacy of your neighbors—it is rude. Do not steal Internet access—it is wrong" (Shiv Polarity 2003, 6).

A third minor theme prevalent in the data involves the creation of collateral damages through policies and practices that invade privacy (n = 23; 10.60 percent). Most of the arguments pertaining to this topic involve policies such as the War on Drugs, the War on Terror, and other measures that inflate the security and surveillance state, primarily in the United States. Searching for offenders of various sorts, these policies cast a wide net of surveillance and cause unwarranted intrusions in the lives of individuals. These efforts are said to be not effective or not worth the cost. Perhaps Goldstein (2002, 4) best summarizes this position when he discusses the expanding role of the FBI following 9/11:

> Now, all of a sudden, we no longer have an agency whose sole purpose is to investigate crimes. Their new reason for being is to prevent the crimes in the first place. Splendid, you might say. Anything that helps to stop crime has got to be a good thing, right?.... If you take an extra few minutes and think it through, you may come to the conclusion that this solution may indeed be a worse crime itself.

The precise nature of the collateral damage differs. Some mention abuses of power by those in positions of authority—such as human rights abuses and police corruption and abuse. Others are concerned about false positives in search and surveillance efforts as well as the creation of a general atmosphere of distrust and fear in society. Overall, the increase in surveillance and the other perceived invasions of privacy are said to create effects other than the intended increases in security.

Another minor theme worth noting is the connection of the concept of privacy with notions of freedom and liberty (n = 11; 5.07 percent). Privacy is often legally contested, particularly in the United States where it is not explicitly protected in the Constitution—and is often contended to be a "penumbra" right. As a result, it

could be said that privacy is not necessarily a right or liberty, a notion that hackers seem to contest:

> The last and final thing you can do to protect your anonymity and privacy in the digital age is to stay informed and lobby the lawmakers. Let them know that you are not happy with the changes they are trying to make in regards to your online privacy. Tell your friends, spread the word about these injustices, and take a stand! If everyone stays silent, they will give your digital liberties away. (Pat D. 2011, 54)

The final minor theme discussed in this study is the idea that hackers are made into scapegoats to draw attention away from the real causes of privacy problems (n = 10; 4.61 percent). Bland Inquisitor (2003b, 15) summarizes this perspective:

> Other companies could expand the basic thrust of the technology [honeypots], perhaps into the p2p networks. At that point it would be us, the hacker community, that stands up and tells the world that this is a gross invasion of privacy. Then, pretty much just like the MPAA did to us, all they would conceivably have to say is: "Consider the source, your honor. *Hackers* want this technology stopped. Hackers are criminals. You don't want to side with criminals, do you? We are here to protect the American people from hackers, and we need you to be brave and give us the power to shut these nasty people down."

According to these authors, the real causes of privacy violations are not hackers but rather those in positions of authority—primarily government agents or organizations as well as corporations—that seek to control some domain of technology, typically the Internet.

Discussion

To make sense of the findings presented in this analysis, we turn to the hacker ethic, liberalism, and technolibertarianism, notably crypto-anarchist thought. As previously stated, the hacker ethic involves a systemic ontology, a belief in freedom of information, a hands-on approach to technology, and a sense of technological utopianism (Barbrook and Cameron 2001; Coleman and Golub 2001; Levy 1984; Stallman 2002; Steinmetz and Gerber 2014; Warnick 2004). The language of liberalism is pervasive in descriptions of the hacker ethic, as shown by its emphasis on personal autonomy, free speech, privacy, etc. A body of political though has emerged within technological circles, including the hacker community, which combines liberalism and technological utopianism—i.e., technolibertarianism (Jordan and Taylor 2004). The technolibertarian philosophy of crypto-anarchy, in particular, provides useful insights for understanding hacker perspectives on privacy (Barbrook and Cameron 2001; Frissell 2001; Hughes 2001; Levy 2001; May 2001).

These philosophical approaches are vital for understanding the theme of dualisms. Indeed, although the dualisms presented in this analysis may seem contradictory—after all, how can something be both a protector and a threat to privacy?—they appear easier to understand if one looks at how the objects of inquiry hinge on power. Government is generally viewed as problematic in its varying functions (which is generally consistent with technolibertarianism and libertarianism). The only occasion in which the authors uphold the protective properties of government is when they are mobilized to uphold and reinforce the rights of individuals to have privacy. Essentially, the government is seen as a source of protection only when it can imbue individuals with power over their information; in this sense, government authority is still viewed as problematic unless it is providing citizens with autonomy and control. Of course libertarians, including technolibertarians, may insist that such imbuement is the exact opposite of what the state is inclined to do, which is a sentiment hackers generally seem to share, considering the general pessimism expressed throughout the data.

Although crypto-anarchists come off as technological utopians, they still recognize that technology can be coopted and used as a tool of power and control (Hughes 2001; May 2001). As a result, individuals must engage in protecting themselves—i.e., they must be personally responsible for their own information—and they can use technology as a means to protect themselves, primarily through cryptography. As crypto-anarchist Hughes (2001, 82) has stated, "We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy out of their beneficence." To understand this perspective, it is useful to draw from a concept that has been given special attention from an anarchist perspective (Ferrell 2001) but is equally applicable to technolibertarian thought, with its liberal emphasis on personal autonomy: the do-it-yourself mentality, which Levy (1984) refers to as the hands-on imperative. Being responsible for one's own privacy is a belief strongly tied to crypto-anarchy, as described by Hughes (2001, 82):

> We must defend our own privacy if we expect to have any. We must come together and create systems that allow anonymous transactions to take place. People have been defending their own privacy for centuries with whispers, darkness, envelopes, closed doors, secret handshakes, and couriers. The technologies of the past did not allow for strong privacy, but electronic technologies do.

Unless individuals take action to protect their privacy (primarily through the use of encryption, but also in other technological domains), this power will shift to the authorities that own, control, and develop technology in people's absence—such as the state and capital. The do-it-yourself mentality also encourages hackers to take an active role in the protection of privacy—by finding vulnerabilities, resisting efforts to restrict privacy, and educating others.

As for the responsibility of owners of data systems to protect personal information, an interesting contradiction emerges within the logic of technolibertarianism and crypto-anarchy. For crypto-anarchists, one reason for the widespread use of cryptography is the protection of free-market enterprise. For instance, May (2001) advocates for encryption to secure communications between virtual communities and to put them ideally on a par with the power of the state, and he specifically includes corporations as one such community. At the same time, however, hackers express concern about the ability of organizations, including corporations, to protect private data. In other words, the laissez-faire liberalism of technolibertarians and crypto-anarchists advocates for the protection of free markets but is dubious when the commodity that is exchanged in the market is personal and potentially sensitive information.

In line with the technolibertarian mistrust of all forms of control from above, hackers also often advocate for the disruption of state and corporate secrecy. Privacy is not for those in positions of power. However, the mistrust of corporate secrecy presents a contradiction similar to the one concerning corporate responsibility toward data retention. Indeed, corporations are responsible for protecting individual privacy but should not be allowed to hold secrets. Here we find competition between liberalism and some features of the hacker ethic. The philosophy of liberalism mandates that corporations should protect personal privacy to uphold individual autonomy (though this may not be as straightforward under neoliberalism). The systemic ontology of the hacker ethic, however, dictates that corporations should seldom be permitted to hold secrets. As Warnick (2004) illustrates when he describes the hacker ontology with the phrase "the world is a computer," this perspective asserts that all systems (technological, social, etc.) function best when information can flow freely, much like the optimal condition for a computer. Secrecy, by contrast, obstructs the ability of information to flow freely. Here, personal privacy, autonomy, and the idea that information wants to be free clash with each other, a disjuncture that seems to hinge on power. Individuals are given more information protection as a mandate of liberalism, whereas more powerful corporations (and the state) are afforded little under the constraints of the "world is a computer" ontology.

The authors also seem to resist the retention of data and the centralization of databases, particularly under the control of the state, as well as the legislated coercion of surveillance capabilities on business. This resistance against the state accumulation of data is wholly consistent with technolibertarianism and its resistance to state control and intrusions into the technological realm. For instance, consider the words that John Perry Barlow (2001, 28), guru of early technolibertarianism, wrote following the creation of the Telecommunications Act of 1996:

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You

> have no sovereignty where we gather. We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us, nor do you possess any methods of enforcement we have true reason to fear.

Here, Barlow rejects the need for the state in virtual realms, referring to state control as tyrannical. Therefore, it is not difficult to see how the centralization and the amassing of resources, including information, under the state (or any form of authority, really) would be viewed as problematic—something with which the authors of *2600* seem to concur.

As mentioned previously under the theme of hacker exemptions, there is another contradiction in the data that needs reconciliation. The authors of *2600* argue for the sanctity of privacy yet also discuss the violation of others' privacy. Such violations are justified on the grounds of exploration, curiosity, and/or the need to find security vulnerabilities. Some of these justifications indicate that hackers do what they do for a degree of enjoyment or thrill (see also Söderberg 2008; Turgeman-Goldschmidt 2005). This activity is similar to the type of transgressive behaviors described by cultural criminologists (Ferrell, Hayward, and Young 2008). Transgressions are acts directed at violating norms, often criminal laws, and are often intimately tied with dynamics of identity, resistance, and lived experience. Intrusion into networks—including instances that may invade others' privacy—can be considered an activity that resists technology laws at the same time as it provides thrills for hackers. In this sense, such intrusions and trespasses may be seen as a celebration of individual autonomy and an exercise of individual power and control encouraged by technolibertarianism.[4] (Future research may want to consider analyzing hacker intrusions from such a perspective; see for example Coleman and Golub 2008.)

Conclusion

Examining hacker perspectives reveals that rather than existing as malicious creatures floating in the digital nether ready to pilfer anyone's information coffers, as their social representation suggests (Halbert 1997; Holt 2009; Skibell 2002; Taylor 1999; Thomas 2005; Yar 2013), hackers, or at least the writers of *2600*, share an underlying philosophical and cultural commitment. Seeing their perspectives on privacy as a result of various manifestations of liberalism and components of the hacker ethic may help explain why hackers engage in privacy violations (e.g., heavy emphasis on autonomy, hands-on imperative, transgression, etc.). This also indicates that hackers have vested interests in privacy and may also be an asset in its protection—for example through exploring, isolating, and reporting vulnerabilities to security systems.

Much like any other study, however, the research presented here also has limitations. One is that *2600* is only one of many possible hacker zines that could have been selected for analysis. Different results may have emerged from other zines. However, *2600: The Hacker Quarterly* enjoys a wide circulation and has been one of the longest running zines. As such, the results from this study may not be representative of the entire hacker subculture, but they may at least represent a sizable population. Second, *2600* is primarily focused on US hacker culture, though international readership and authorship are not uncommon. Hacking, however, has increasingly become an international phenomenon, and future research should incorporate more international data. A third limitation is that there is the possibility that editorial bias (i.e., the selection of certain themes and perspectives by the journal's editors) influenced the results. Future research can control for this by looking across other publications and/or at alternate forms of data—like field research, for example. Because *2600* is so widely circulated, however, the potential editorial bias may still reflect sentiments shared in the broader hacking community.

A fourth limitation springs from the type of data used—published items in a publicly available zine. As a result, only those views that the authors saw fit for publication were published, which may not convey the totality of the authors' perspectives on privacy. However, it should be noted that many of the authors used handles or pseudonyms to obscure their identities, and such attempts at anonymity may indicate a higher propensity to divulge one's actual feelings about privacy. Fifth, letters to the editor were omitted from this study. Different or perhaps more robust findings might have been found from an analysis of these items, as inclusion of these letters would allow the inclusion of perspectives of readers who either do not write well enough to have a piece published or do not care to submit an item for publication. Future content analyses may want to consider including these items as well as additional sources of data.

In conclusion, the present study is only an initial exploration of hacker perspectives on privacy. Future analyses should probe these perspectives further and also consider how they might affect other areas of hacker culture and behavior.

NOTES

1. The authors of this study recognize that many other controversies have occurred in recent times and do not mean to diminish these events through their exclusion from this manuscript. They are only omitted for the sake of brevity. For readers interested in specific accounts of intrusions and other hacker engagements, numerous works may prove valuable (e.g., Jordan and Taylor 2004; Thomas 2002). The authors would like to thank Reviewer #2 for his generous explications of recent hacker accounts related to our analysis.

2. A zine is a self-published magazine, tipically with a small circulation amongst a niche population. The authors of the articles published in *2600* are largely assumed to be hackers. It is entirely possible, however, that articles were written by people who do not consider themselves hackers or are

not considered as such by the hacker community at large. In order to avoid confusing terminology and unnecessary ambiguity, this analysis treats all authors as hackers.

3. Pseudonyms are often used to provide some level of anonymity for the writers. As a result, it is impossible to provide a breakdown of the demographic characteristics of the authors. Identifying characteristics like gender, race, age, and geographic location would be an act of speculation at best. The reader should be aware that although the zine has a global reach, the audience seems to be largely based in the United States.

4. The thrills and trespassings may also be related to a kind of hacker masculinity linked to a Wild West mentality of online frontiersmanship (Jordan and Taylor 2004). Although this paper only looks at motivations for hacker behavior from the perspective of technolibertarianism, other explanations also exist (see Turgeman-Goldschmidt 2005).

REFERENCES

Acrobatic
2012 "Learning from Stratfor: Extracting a Salt from an MD5 Hash." *2600: The Hacker Quarterly* 29(1): 49–51.

area_51
2002 "CBDTPA: Another Privacy Concern." *2600: The Hacker Quarterly* 19(2): 54–55.

Bachmann, Michael
2010 "Deciphering the Hacker Underground: First Quantitative Insights." In *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications,* edited by Thomas J. Holt and B. H. Schell, 105–26. Hershey, PA: IGI Global.

Barbrook, Richard and Andy Cameron
2001 "California Ideology." In *Crypto Anarchy, Cyberstates, and Pirate Utopias,* edited by Peter Ludlow, 363–88. Cambridge, MA: MIT Press.

Bland Inquisitor
2002a "Telezapper, Telemarketers, and the TCPA." *2600: The Hacker Quarterly* 19(3): 11–12.
2002b "Honeypots: Building the Better Hacker." *2600: The Hacker Quarterly* 19(4): 15–16.

b0rn_slippy
2006 "More on Hacking Facebook." *2600: The Hacker Quarterly* 23(2): 7–11.

Bossler, Adam M. and George W. Burruss
2010. "The General Theory of Crime and Computer Hacking: Low Self-Control Hackers?" In *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications,* edited by Thomas J. Holt and B. H. Schell, 38–67. Hershey, PA: IGI Global.

Brown, Barrett
2008 "The State of Cyberspace and Cyberwar." *2600: The Hacker Quarterly* 25(3): 10–11.

bTrack3r2003
2011 "Laptop Repair, Customer Beware." *2600: The Hacker Quarterly* 28(4): 25.

Charmaz, Kathy
2002 "Qualitative Interviewing and Grounded Theory Analysis." In *Handbook of Interview Research: Context & Method*, edited by J. F. Gubrium and James A. Holstein, 675–94. Thousand Oaks, CA: Sage.

Charmaz, Kathy
2006 *Constructing Grounded Theory: A Practical Guide through Qualitative Analysis*. Thousand Oaks, CA: Sage.
Clarke, Adele E.
2005 *Situational Analysis: Grounded Theory after the Postmodern Turn*. Thousand Oaks, CA: Sage.
Coleman, Gabriella E.
2010 "The Hacker Conference: A Ritual Condensation and Celebration of a Life-world." *Anthropological Quarterly* 83(1): 47–72.
2012 "Phreakers, Hackers, and Trolls and the Politics of Transgression and Spectacle." In *The Social Media Reader,* edited by Michael Mandiberg, 99–119. New York: NYU Press.
2013 *Coding Freedom: The Ethics and Aesthetics of Hacking*. Princeton, NJ: Princeton University Press.
Coleman, Gabriella E. and Alex Golub
2008 "Hacker Practice: Moral Genres and the Cultural Articulation of Liberalism." *Anthropological Theory* 8(3): 255–77.
docburton
2002 "Your Eyes Have Just Been Sold." *2600: The Hacker Quarterly* 19(2): 40–43.
Dragorn
2007 "Transmissions." *2600: The Hacker Quarterly* 24(4): 52–53.
2010 "Transmissions." *2600: The Hacker Quarterly* 27(2): 52–53.
Eberhard, Martin
2008 "Hacker Perspective." *2600: The Hacker Quarterly* 25(1): 26–28.
Ferrell, Jeff
1993 *Crimes of Style: Urban Graffiti and the Politics of Criminality*. Boston, MA: Northeastern University Press.
2001 *Tearing Down the Streets: Adventures in Urban Anarchy*. New York: Palgrave.
Ferrell, Jeff, Keith Hayward, and Jock Young
2008 *Cultural Criminology: An Invitation*. Thousand Oaks, CA: Sage.
Frissell, Duncan
2001 "Re: Denning's Crypto Anarchy." In *Crypto Anarchy, Cyberstates, and Pirate Utopias,* edited by Peter Ludlow, pp. 105–14. Cambridge, MA: MIT Press.
Furnell, Steven
2010 "Hackers, Viruses and Malicious Software." In *Handbook of Internet Crime,* edited by Yvonne Jewkes and Majid Yar, pp. 173–93. Portland, OR: Willan Publishing.
Garland, David
2002 *The Culture of Control: Crime and Social Order in Contemporary Society.* Chicago: University of Chicago Press.
Goldstein, Emmanuel
2002 "Fair Use and Abuse." *2600: The Hacker Quarterly* 19(2): 4–5.
2006 "Whom Shall We Blame." *2600: The Hacker Quarterly* 23(2): 4–5.
2008 "The Whole World's Watching." *2600: The Hacker Quarterly* 25(1): 4–5.
2009 "Smart Regression." *2600: The Hacker Quarterly* 26(4): 2–3.
Halbert, Debora
1997 "Discourses of Danger and the Computer Hacker." *The Information Society* 13(4): 361–74.
Himanen, Pikka
2001 *The Hacker Ethic: A Radical Approach to the Philosophy of Business*. New York: Random House.

Hollinger, Richard
1991 "Hackers: Computer Heroes or Electronic Highwaymen?" *Computers & Society* 21(1): 6–17.
Holt, Thomas J.
2009 "Lone Hacks or Group Cracks: Examining the Social Organization of Computer Hackers." In *Crimes of the Internet,* edited by Frank Schmalleger & Michael Pittaro, 336–55. Upper Saddle River, NJ: Pearson Education.
2010a "Becoming a Computer Hacker: Examining the Enculturation and Development of Computer Deviants." In *In Their Own Words: Criminals on Crime: An Anthology*, edited by P. Cromwell, 109–23. 5th ed. Los Angeles: Roxbury Publishing.
2010b "Examining the Role of Technology in the Formation of Deviant Subcultures." *Social Science Computer Review* 28(4): 466–81.
Hughes, Eric
2001 "A Cypherpunk's Manifesto." In *Crypto Anarchy, Cyberstates, and Pirate Utopias,* edited by Peter Ludlow, 81–83. Cambridge, MA: MIT Press.
Jordan, Tim and Paul Taylor
1998 "A Sociology of Hackers." *The Sociological Review* 46(4): 757–80.
2004 *Hacktivism and Cyberwars: Rebels with a Cause*. New York: Routledge.
Levy, Steven
1984 *Hackers: Heroes of the Computer Revolution*. New York: Penguin Group.
2001 *Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age*. New York: Penguin Group.
Lifeguard
2011 "What is a Hacker?" *2600: The Hacker Quarterly* 28(1): 16.
Malf0rm3dx and Megalos
2011 "Air Intercepted Messaging: A Revisit of POCSAG and Radio Privacy Issues." *2600: The Hacker Quarterly* 28(2): 29–32.
malpelo93
2008 "Bank of America Website Flaw Allows Reading of Other Customers' Statements." *2600: The Hacker Quarterly* 25(2): 55.
May, Timothy C.
2001 "The Crypto Anarchist Manifesto." In *Crypto Anarchy, Cyberstates, and Pirate Utopias,* edited by Peter Ludlow, 61–63. Cambridge, MA: MIT Press.
McKenzie, Jon
1999 "!nt3rh4ckt!v!ty." *Style* 33(2): 283–99.
Meikle, Graham
2002 *Future Active: Media Activism and the Internet*. New York: Routledge.
Morris, Robert G.
2010 "Computer Hacking and Techniques of Neutralization." In *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications,* edited by Thomas J. Holt and Bernadette H. Schell, 1–17. Hershey, PA: IGI Global.
Newman, Jared
2013 "The Target Credit Card Breach: What You Should Know." *Time*, December 19. At *http://techland.time.com/2013/12/19/the-target-credit-card-breach-what-you-should-know/*.
Nichols, Randall K, Daniel J. Ryan, and Julie J.C.H. Ryan
2000 *Defending Your Digital Assets against Hackers, Crackers, Spies, and Thieves*. New York: McGraw-Hill.
OSIN
2007 "Power Trip." *2600: The Hacker Quarterly* 24(4): 6–8.

Pat D.
2011 "Anonymity and the Internet in Canada." *2600: The Hacker Quarterly* 28(4): 54.
p4nt05
2010 "Outline for a Simple Darkserver and/or Darknet." *2600: The Hacker Quarterly* 27(2): 46–48.
Schell, Bernadette H.
2010 "Female and Male Hacker Conferences Attendees: Their Autism-Spectrum Quotient (AQ) Scores and Self-Reported Adulthood Experiences." In *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications,* edited by Thomas J. Holt and Bernadette H. Schell, 144–68. Hershey, PA: IGI Global.
Schell, Bernadette H. and Thomas J. Holt
2010 "A Profile of the Demographics, Psychological Predispositions, and Social/Behavioral Patterns of Computer Hacker Insiders and Outsiders." In *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*, edited by Thomas J. Holt and Bernadette H. Schell, 190–213. Hershey, PA: IGI Global.
Shiv Polarity
2003 "Getting to Know Your Neighbors." *2600: The Hacker Quarterly* 23(3): 6–8.
Skibell, Reid
2002 "The Myth of the Computer Hacker." *Information, Communication & Society* 5(3): 336–56.
Söderberg, Johan
2008 *Hacking Capitalism: The Free and Open Source Software Movement*. New York: Routledge.
Stallman, Richard
2002 *Free Software Free Society: Selected Essays of Richard M. Stallman*. Boston, MA: Free Software Foundation.
Steinmetz, Kevin F.
2012 "WikiLeaks and Realpolitik." *Journal of Theoretical and Philosophical Criminology* 4(1): 14–52.
Steinmetz, Kevin F. and Jurg Gerber
2014 "'The Greatest Crime Syndicate Since the Gambinos': A Hacker Critique of Government, Law, and Law Enforcement." *Deviant Behavior* 35(3): 243–61.
Strauss, Anselm L. and Juliet Corbin
1998 *Basics of Qualitative Research: Grounded Theory Procedures and Techniques*. 2nd ed. Thousand Oaks, CA: Sage.
The Prophet
2002 "A New Era of Telecommunications Surveillance." *2600: The Hacker Quarterly* 19(2): 23–25.
2009 "Telecom Informer." *2600: The Hacker Quarterly* 26(1): 13–14.
Thomas, Douglas
2002 *Hacker Culture*. Minneapolis: University of Minnesota Press.
Thomas, Jim
2005 "The Moral Ambiguity of Social Control in Cyberspace: A Retro-Assessment of the 'Golden Age' of Hacking." *New Media & Society* 7(5): 599–624.
Turgeman-Goldschmidt, Orly
2005 "Hackers' Accounts: Hacking as a Social Entertainment." *Social Science Computer Review* 23(1): 8–23.

Turgeman-Goldschmidt, Orly
2011 "Identity Construction among Hackers." In *CyberCriminology: Exploring Internet Crimes and Criminal Behavior,* edited by K. Jaishankar, pp. 31–51. Boca Raton, FL: CRC Press.

Van Laer, Jeroen and Peter Van Aelst
2010 "Cyber-Protest and Civil Society: The Internet and Action Repertoires in Social Movements." In *Handbook of Internet Crime,* edited by Yvonne Jewkes and Majid Yar, 230–54. Portland, OR: Willan Publishing.

Warnick, Bryan R.
2004 "Technological Metaphors and Moral Education: The Hacker Ethic and the Computational Experience." *Studies in Philosophy and Education* 23(4): 265–81.

Woo, Hyung-Jin, Yeora Kim, and Joseph Dominick
2004 "Hackers: Militants or Merry Pranksters? A Content Analysis of Defaced Web Pages." *Media Psychology* 6(1): 63–82.

Xyzzy
2007 "Security Holes at Time Warner Cable." *2600: The Hacker Quarterly* 24(1): 19–20.