CRI CHRISTIAN RESEARCH INSTITUTE
PO Box 8500, Charlotte, NC 28271

Feature Article: **JAF1371**

HEROES OR VILLAINS?
A CHRISTIAN ASSESSMENT OF HACKTIVISM

by Douglas Groothuis

This article first appeared in the CHRISTIAN RESEARCH JOURNAL, volume 37, number 01 (2014). For further information or to subscribe to the CHRISTIAN RESEARCH JOURNAL go to: http://www.equip.org/christian-research-journal/

Is it the most freeing element of the Internet, liberating data, exposing lies, speaking truth to power, or is it the most corrupt and corrupting side of cyberspace, stealing data, telling secrets, endangering citizens, and seeking fame through theft? Or is it something in between? I am writing of hacktivism—a term that is hard to define, even though it is popping up everywhere. Parmy Olson, an expert and author on hacktivism, defines hacktivists as "hackers with an activist message."[1]

The term hacktivism is obviously taken from *hacking* and *activism*. Originally, hacking tended to refer to collaborative or "open source" work on programs such as Linux. The program was not proprietary to any one company, unlike the computer code used for Microsoft products. But hacking can also mean the unauthorized mining of data from the Internet through technological savvy. Hacking always has been a mixture of the innocuous and the subversive. Steve Jobs and Steve Wozniak, cofounders of Apple, found a way to make long-distant calls for free and to sell this know-how to others.[2] This "phone phreaking" is a straightforward case of stealing, which the Bible condemns (Exod. 20:15; Mark 10:19). The first case of "identity theft" is when Jacob pretended to be Esau in order to receive the blessing of their father, Isaac (Gen. 27; see also Gen. 29). However clever he was, Jacob was not virtuous.

After consulting the first forty book offerings on "hacking" at Amazon.com, I found no book offering a *moral* critique of it. Rather, all forty were *guides* to hacking: *Hacking for Dummies* (of course), and numerous titles on hacking specific programs and applications, such as hacking Kindle Fire (a portable reading device). This is a bit odd, since Amazon (which makes Kindle Fire) was selling the book and even offers it on Kindle.

Having considered hacking, let us consider hacktivism in more detail. Hacktivists are technologically skilled users who acquire information through means not designed by the data's controllers. This data is then used to promote some moral or political cause. Their activities are often meant to derail governmental surveillance, which they take to be intrusive or even authoritarian. Hacktivism can be deemed cyber warfare.

Consider the boiling controversy over the young National Security Agency (NSA) worker Edward Snowden, who illegally released classified data taken by the United States government in order to expose what he took to be intrusive intelligence gathering. While a hero to some, he had to flee his country and has (as of this by Douglas Groothuis writing) found temporary asylum abroad in Russia.

WikiLeaks, headed by the Australian Julian Assange, has also sparked global attention for such actions as stealing and releasing classified military information from the U.S. government, including, in 2010, details of operations in the war in Afghanistan. Here is a sample statement from their web page, dated October 24, 2012: "WikiLeaks has begun releasing the 'Detainee Policies': more than 100 classified or otherwise restricted files from the United States Department of Defense covering the rules and procedures for detainees in U.S. military custody."[3]

It does not take an expert on foreign policy to realize the implications that the public release of this kind of classified information would have on military and diplomatic affairs for any government in question. WikiLeaks has leaked information from the Peruvian and Canadian governments as well. As such, they pose a global threat to the security of nations.

Cases of obvious wrongdoing occurred when organized crime discovered it could siphon away millions of dollars from banks by hacking into their computers. Hackers could also be tricksters and pranksters, sabotaging the Internet more in jest than in earnest. Yet this power was alluring. The activism of hacktivism may be malignant. The *New York Times* noted, "At a time when life, commerce and statecraft have gone digital, hacktivists can threaten governments, or they can just as easily dump innocent people's credit card numbers on the Internet for more common criminals to steal."[4]

But hacking was usually taken to mean the acquiring of off-limits data for one's own private use or perhaps for a small group. Hacktivism, on the other hand, usually claims (rightly or wrongly) a moral authority for the common good. Its targets may be national governments or large organizations of various kinds. Hacktivists may seek to liberate data made secret or to shut down a web page. Some hacktivists even threatened to shut down the entire Internet in April of 2012.

One hacktivist, Sabu—often involved in criminal hacking—tweeted this humble statement: "Give us liberty or give us death—and there's billions of us around the world. You can't stop us. Because without us you won't exist." Sabu, AKA Hector Xavier Monsegur, is now on the run from the authorities.[5]

A group named Anonymous is made up of a closely associated group of hackers scattered around the planet. It has claimed to lead a global Internet insurgency by hacking into federal computer systems and other underground cyberspace activities. They "posted their ominous tagline on blogs, hacked websites, or wherever they could:

We are Anonymous
We are Legion
We do not forgive

We do not forget
Expect us." [6]

One could go on about the assorted aspects of hacktivism. While it is a developing, multifaceted, and somewhat fragmented movement, it demands our attention and moral discernment, since it is not going away and will likely gain in strength as technologies continue to fight each other.

First, hacktivism should be placed in a larger historical and theological context. Ever since the fall, humans have kept secrets from each other. Our first parents tried to hide from God and then tried to hide their blame for their sin (Gen. 3:1– 13). Secrecy and the desire to break secrecy both stem from human sin. If love and truth had prevailed on Earth, there would be no desire to cover up or uncover anything. Alas, this is not our lot under the sun. God, in His power and goodness, elects to keep His secrets, but this does not issue from sin but from His eternally wise counsel (Deut. 29:29; Eccl. 8:17–18; Rom. 11:33–36). No secrets need be kept or stolen in the new heaven and new earth, since the curse is removed, and God's presence is perfectly obvious to the redeemed (Rev. 21–22).

Second, in this world east of Eden, some secrets are morally justified and should not be stolen. Some knowledge is property (as in what is copyrighted or patented) and belongs only to its owner. This is because evildoers may use the truth immorally. Therefore we put locks on our doors and have passwords for the Internet. Not everyone has the right to know how to get in without our permission. One may covet knowledge that one does not deserve or have a right to possess. Since people are sinful, and hurt others with truth, we need privacy, as with our medical and financial records. Further, secrecy is paramount in warfare. Information is encoded and decoded; weapons are camouflaged; and spies do necessary work.[7] British wartime leader Winston Churchill said, "In wartime truth is so precious that she should be attended by a bodyguard of lies." But even that may now be impossible, as a British journalist notes: "Whatever good and bad has come from WikiLeaks' publication of operational secrets, this episode provides further proof that in the age of the web, 24-hour news, the ubiquitous mobile phone and a digital camera in everyone's hands, Churchill's bodyguard of lies is no longer available in the 21st century."[8]

Third, the state commands a God-given authority, "the power of the sword," in order to punish wrongdoers and protect the innocent (Rom. 13:1–7; 1 Pet. 2:25). As such, the civil government must sometimes keep military and other secrets, since public disclosure could aid criminals or foreign enemies. The state sometimes needs to monitor its own citizens secretly, especially in an age of terrorism, more of which is homegrown. This, of course, can be easily abused in the hands of unaccountable power. The NSA has come under heavy attack in this regard, especially since the leaking of documents by Edward Snowden. "The eye-catching success of WikiLeaks will inspire further betrayal of privileged information by government officials, and will increase the dangers to our forces fighting what these reports graphically portray to be an already highly lethal and chaotic war."[9]

This is the dangerous side of hacktivism, which can become anarchistic and thus destructive of social order. Hacktivists may betray necessary secrets and cause unnecessary mayhem and loss of life. However, the civil government may transgress objective moral boundaries in its surveillance on its citizens. George Orwell describes this artfully in his novel *1984*, where freethinking people must rebel against the tyrannical party. Hence resistance is the way to restore liberty and dignity for a people oppressed through spying. Scripture teaches that while higher authorities are needed in a fallen world, those authorities may go radically wrong. Pharaoh oppressed God’s people and would not let them go (Exod.). Two Hebrew midwives resisted Pharaoh’s agents of death when they told Shiphrah and Puah to murder the Hebrew babies (Exod. 1:15–21). Herod accepted praise that hailed him as a deity, and was struck down by God Himself (Acts 12). Jesus taught that Caesar had limited jurisdiction: “Render therefore unto Caesar the things which are Caesar’s; and unto God the things that are God’s” (Matt. 22:21 KJV).

Reasoning through the causes and limits of civil disobedience is no simple matter, but it is called for on some occasions because the state may become a beast (Rev. 13). Perhaps if a civil government usurps the rights of its citizens through illegal surveillance, it becomes permissible to engage in civil disobedience through hacktivism.[10] This should be viewed as a last resort under extreme conditions, since the risks are so high that one might be betraying important national secrets at home or abroad. Or people may simply take the law into their own hands. The *Huffington Post* revealed that Derrick Lostutter “was raided by the FBI after he and other members of Anonymous got involved in a rape case in Steubenville, Ohio, that gained national attention in late 2012. When two members of a high school football team in the city were accused of raping a 16-year-old girl, Anonymous members did not think the case was getting enough attention and leaked information about people they believed were involved.”[11]

This is nothing but vigilantism, and should be avoided as morally wrong.[12] Nor may the Christian engage in hacktivism uncritically or to display mere technical skill. This is poor stewardship and may, in fact, be rightly criminal. As Paul says, “But if you do wrong, be afraid, for rulers do not bear the sword for no reason. They are God’s servants, agents of wrath to bring punishment on the wrongdoer” (Rom. 13:4).

Warnings of this caliber ought to be taken seriously, and the burden of proof is on the one who breaks the law for the sake of a higher law or “the law above the law.”[13] Nevertheless, in a fallen and often unjust world, this must be considered. Ecclesiastes drives home this sad point: “Again I looked and saw all the oppression that was taking place under the sun: I saw the tears of the oppressed—and they have no comforter; power was on the side of their oppressors—and they have no comforter” (Eccl. 4:1 NIV).

In the power and wisdom of God, we should seek to be the comforters of the oppressed, including those oppressed by tyrannical uses of the Internet. In some cases, for the sake of justice, we need to fight fire with fire—but we must avoid burning up a godly conscience in the process. However, developing a robust theory of what principled hacktivism consists of requires more research and thinking than what this article can offer.[14] May Christians lead the pack in thinking hard and acting wisely concerning this emerging moral issue.

Douglas Groothuis is professor of philosophy at Denver Seminary and heads the apologetics and ethics master's program.

NOTES

[1] Parmy Olson, *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency* (New York: Back Bay Books, 2012), 6.

[2] Geeta Daya, "Freaks and Geeks: Before Steve Jobs and Steve Wozniak Invented Apple, They Hacked Phones," *Slate*, Feb. 1, 2013. See also Walter Isaacson, *Steve Jobs* (New York: Simon and Schuster, 2011), 27–30.

[3] "Detainees Policy," WikiLeaks.org, http://www.wikileaks.org.

[4] Somini Sengupta, "The Soul of the New Hacktivist," *New York Times*, March 17, 2012.

[5] N. R. Kleinfield and Somini Sengupta, "Hacker, Informant and Party Boy of the Projects," *New York Times*, March 8, 2012.

[6] Olson, *We Are Anonymous*, 7.

[7] On spying in the Bible, see Numbers 13–14 and Joshua 1–2.

[8] Richard Kemp, "WikiLeaks: The End of Churchill's Bodyguard of Lies," *The Guardian*, July 25, 2010, http://www.theguardian.com/commentisfree/2010/jul/26/wikileaks-end-churchills-bodyguard-of-lies.

[9] Ibid.

[10] On civil disobedience, see Francis A. Schaeffer, *A Christian Manifesto* (Wheaton, IL: Crossway, 1981); Martin Luther King, Jr., *Why We Can't Wait* (1963; Boston: Beacon Press, 2010).

[11] Betsy Isaacson, "7 Anonymous Hackers Who Have Been Unmasked," *The Huffington Post*, June 7, 2013, http://www.huffingtonpost.com/2013/06/07/ anonymous-hackers_n_3398282.html.

[12] See Les Johnston, "What Is Vigilantism?" *The British Journal of Criminology* 36, 2 (1996): 220–36.

[13] See John Warwick Montgomery, *The Law above the Law* (Minneapolis: Bethany Fellowship, 1975).

[14] To my knowledge, little has been written on hacktivism from a Christian viewpoint.