

---

By TOM CROSS

---

# ACADEMIC FREEDOM AND THE HACKER ETHIC

*Hackers advocate the free pursuit and sharing of knowledge without restriction, even as they acknowledge that applying it is something else.*

T

here is a global culture of people who call themselves computer hackers that is driven by a fundamental belief that information should be free and that the pursuit of knowledge is an essential human right. Most hackers seek to do creative things with technology, but the community is often beset by controversy because it centers on forbidden knowledge; in particular, hackers like to think about how computer security fails. The general public often has difficulty drawing a line between hackers who study computer security as a technical interest and criminals who break into computers and deliberately cause damage. Some observers in the media and the academic community have argued that the sort of information hackers discuss at conferences and in journals should never be shared publicly, saying that knowledge is itself dangerous, irrespective of the motives of the people discussing it.

Controversy involving the hacker community is analogous to new fears being raised about science in general. In the past decade academic and policy circles have begun discussing the idea that as technology advances and laboratory equipment becomes less costly and easier to access, rogue scientists may be able to use their knowledge to harm people, either through accidents or by intentionally crafting dangerous weapons. Sun Microsystems co-founder Bill Joy is often viewed as leading this charge, following his famous essay “Why the Future Doesn’t Need Us” [3] in which he argued that advancements in biology, nanotechnology, and robotics will soon give rise to technological capabilities beyond our control, threatening the survival of all humanity. He proposed that we “relinquish” the pursuit of entire classes of scientific knowledge in order to avoid a catastrophe. Over time, it has become increasingly evident that a broad policy debate about academic freedom is taking form in which the perspective of the hacker community may represent a critical counterweight to overzealous calls for control of the pursuit of knowledge.

You can see the clouds of this debate gathering in recent controversies in biotechnology. Governments worldwide have passed regulations intended to control advanced biotech products and research deemed risky or inhumane. For example, the European Union banned new genetically modified crops for five years ending in 2003, and six African governments have refused to accept genetically modified food aid. In August 2005, the U.N. issued a declaration banning human cloning. Debate has raged in North America about the moral implications of stem cell research. Biological advances scare some of us because we are unsure of the morality of tampering with the fundamentals of life and because we are worried about the unforeseen consequences of releasing organisms into the natural environment after they’ve been modified by humans.

It seems clear that advances in other fields (such as nanotechnology and artificial intelligence) will eventually bring us self-reproducing machines that involve many of the same problems. Many of the arguments being made today in the context of bioethics are broad enough that they can also encompass these future developments, threatening to produce regulations that deeply affect our personal and professional academic freedom.

Francis Fukuyama, an influential U.S. political economist and a member of the U.S. President’s Council on Bioethics, published an essay in 2002 [1] laying out a set of philosophical arguments for government control of basic research, even when pursued

outside the federal grant system. He wrote that “Science itself is just a tool for achieving human ends; the political community must decide which ends to pursue.” This idea strikes at the heart of academic freedom. Our universities have certain institutional structures (such as the tenure system) specifically designed to shield basic research from the sort of political influence Fukuyama advocated. These structures exist to enable human knowledge to expand toward every opportunity for growth and for the discovery of truth without being hampered by fear and special interests. Fukuyama’s perspective represents a fundamental challenge to our society’s overall approach to the advancement of science.

How should the scientific community respond? Should it embrace regulations that prohibit publication of certain kinds of technical information? Should it advocate that national governments require approval for private research projects? Should it pass laws prohibiting scientists from examining certain subjects or developing certain technologies? The hacker community would say no. From grappling with these questions over the years, hackers have developed a nuanced and sophisticated understanding of the line between ideas and actions, as well as the dangers posed by allowing governments to control what people are allowed to think about, particularly with regard to scientific or technical inquiry. Their perspectives on these issues, and the lessons they’ve learned responding to critics and working to resist overzealous legislation are a necessary ingredient when considering these questions.

Hackers believe that ethical questions generally apply to the application of knowledge rather than to the pursuit of knowledge. While ethical questions arise in scientific study, they usually relate to ensuring that people are not harmed by experiments rather than whether the knowledge being sought is harmful in and of itself. Knowing how to do something that might be harmful is not the same as causing harm. Once you have knowledge you still must decide what to do with it. For example, if you know how to pick a lock, you can apply that knowledge as a locksmith, troubleshooting lock problems and designing better locks, or you can apply that knowledge as a thief. You can witness this distinction in action at hacker conferences like Defcon where attendees draw a line between “white hats” trying to improve the state of computer security and “black hats” trying to upend it. Both groups are interested in the same sort of knowledge. The moral distinction comes from how they apply it.

Hackers reject the notion that ignorance makes you safer. In the 1980s, as computer networks grew and computer security problems grew with them, vendors, government agencies, and university labs kept software vulnerabilities secret from the general public, even as they quietly shared information with one another. Computer criminals developed their own independent techniques they shared within their own networks. Left in between were large numbers of people responsible for operational Internet systems who were not part of either community and were largely in the dark about how to protect themselves.

Most people who openly discussed computer vulnerabilities at the time belonged to the hacker community. Partly out of frustration with the status quo, they began “full disclosure” email lists where vulnerability details were discussed in plain view of the general public, usually after software patches had been released. Today, these lists represent a cornerstone of the professional computer security world. This open dialogue has been positive for computer security; the ability to understand and share research findings and learn from the mistakes of others makes security practitioners smarter. Having a smart worldwide community of security practitioners makes end users safer and is well worth the advantage that disclosure might offer unsophisticated attackers unable to develop their own techniques.

Hackers also believe that valuable new ideas do not always come from established institutions. When governments get involved in regulating dangerous knowledge they often overreact by erecting barriers to “amateurs”; for example, the U.S. Digital Millennium Copyright Act of 1998 prohibits research into certain classes of computer security vulnerabilities unless “the person is engaged in a legitimate course of study, is employed, or is appropriately trained or experienced in the field of encryption technology.” These restrictions seem to have been aimed specifically at hackers, as if security research that does not occur in traditional institutions is not worthy of legal protection. This restriction indeed affects the entire computer science community as its members pursue research both personally and professionally.

It is widely understood that critical developments in computer science have come from garages and hobby clubs (most notably the Homebrew Computer Club, an early crucible of the personal computer revolution). Consider the plethora of free and open source software projects that glue the Internet together, many written by amateurs and students. This font of innovation happens in the field of computer security as well. Ask security professionals where they would be without free tools (such as the Nmap

## KNOWING HOW TO DO SOMETHING THAT MIGHT BE HARMFUL IS NOT THE SAME AS CAUSING HARM.

---


port scanner, the NetCat networking utility, and the OllyDbg debugger). All of us would certainly lose a great deal if we deliberately limited science to only a few select laboratories and research institutions.

Most important, hackers believe the pursuit of knowledge is an inalienable right, tied directly to freedom of speech. Individual rights are not important simply because of some idealistic notion of freedom. If government regulators are given the legal authority to decide what questions may be asked and answered, they will have the power to prevent us from discovering the truths that are critical to our interests.

Paul Graham, the creator of bayesian spam filtering, illustrated the connection between civil liberties and technology in a 2004 essay [2] in which he wrote “A society in which people can do and say what they want will also tend to be one in which the most effi-

cient solutions win, rather than those sponsored by the most influential people. Authoritarian countries become corrupt; corrupt countries become poor; and poor countries are weak... This is why hackers worry. The government spying on people doesn't literally make programmers write worse code; it just leads eventually to a world in which bad ideas will win."

In 2005, Bill Joy and Raymond Kurzweil wrote an essay [4] protesting the academic publication of the genome for the 1918 flu, which killed tens of millions worldwide. Fearing that terrorists might use this information to craft biological weapons, they called the publication "extremely foolish" and suggested that the precise genome be shared only "with scientists with suitable security assurances." This sort of argument is too familiar. While the balance of interests and risks in the full disclosure of pathogen genomes is different from those inherent in software vulnerabilities, we cannot give in to fear and presume that the right answer is always as simple as sweeping dangerous information under the rug.

The history of the hacker community is filled with people who have faced significant personal consequences for revealing truths powerful interests sought to suppress. A future in which scientists of all stripes face such pressures and the bulk of human knowledge is kept under lock and key is not the sort of future I want to live in. Government policy makers should manage these risks by controlling access to certain raw materials and regulating practical applications rather than censoring ideas and information. Academic freedom should be restricted only as an absolute last resort, not as the fundamental basis of our national strategies for security and technological development in the 21st century. 

## REFERENCES

1. Fukuyama, F. How to regulate science. *The Public Interest* 146 (Winter 2002); [www.sais-jhu.edu/faculty/fukuyama/articles/pi.pdf](http://www.sais-jhu.edu/faculty/fukuyama/articles/pi.pdf).
2. Graham, P. *The Word Hacker*. Posted on a personal Web site (Apr. 2004); [www.paulgraham.com/gba.html](http://www.paulgraham.com/gba.html).
3. Joy, B. Why the future doesn't need us. *Wired Magazine* 8, 4 (Apr. 2000); [www.wired.com/wired/archive/8.04/joy.html](http://www.wired.com/wired/archive/8.04/joy.html).
4. Kurzweil, R. and Joy, B. Recipe for destruction. *New York Times* (Oct. 17, 2005); [www.ihl.com/articles/2005/10/17/opinion/edkurzweil.php](http://www.ihl.com/articles/2005/10/17/opinion/edkurzweil.php).

---

**TOM CROSS** (tom@memestreams.net) lives in the U.S. where he works in the computer security industry as a vulnerability researcher. He wears a white hat.

---

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

---

