

March 2006

## The Engineering Mind of Winny

Shinji Yamane

Research Fellow

Center for Global Communications (GLOCOM)

International University of Japan.

Founding Board Member

Computer Professionals for Social Responsibility, Japan Chapter.

Center for Global Communications,  
International University of Japan

Harks Roppongi Bldg. 2F, 15-21  
Roppongi 6-chome, Minato-City,  
Tokyo 106-0032 Japan

URL <http://www.glocom.ac.jp/>

TEL +81-3-5411-6677

FAX +81-3-5412-7111

Shinji Yamane made the following remarks on technology and society, and Winny from the point of view of a hacker in response to Isamu Kaneko's presentation at the "Winny Technology and Ethics" symposium, 28 January 2006.

Last year, a graduate student came to consult with me. This person was engaged in research into general-purpose anonymization technologies and was concerned whether he might face an arrest if the system he developed came into widespread public use.

After witnessing the arrest of the engineers engaged in the development of Winny, students conducting research into internet technology and security, with a view to their practical application and use, seem to be feeling anxious and rather insignificant. I advised him not to promote the technology in Japan. At that time no one knew whom to consult about these anxieties and there was no forum for discussing how to solve such problems. In other words, there have been no discussions concerning the engineer's mindset, how experts such as ourselves who are working on Winny and similar technologies can conduct our research, even though discussions concerning the engineering, social and scientific viewpoints of Winny have been held openly and even been dealt with in questions

presented to the Diet. This is the starting point for my remarks.

In general, engineers in overseas and experts in the United States are said to express their opinions actively, unlike their Japanese counterparts. For example, the world's largest academic computer society, the Association for Computing Machinery (ACM), monitors trends in the United States Congress, calls on members to provide them with information, and compiles comments to be included in processes of drafting legislation. However, experts in the United States did not initially watch over these trends, the initiative started only during the 1980s.

In 1984, Richard Matthew Stallman, then a star computer programmer at MIT was quoted in a Newsweek magazine feature article about computer hackers saying that the copyright situation at the time posed severe problems. In response, series of criticisms were published in the academic journals of ACM by the chairman of the society and the editor-in-chief of the magazine. This reaction made Stallman quite famous and his work eventually led to the development of open source software such as Linux. However academic society at the time regarded him as something of a terrorist. Today, the ACM has stated there is no future for the copyright

industry if it fails to deal promptly with new business models. This indicates what a dramatic generational change has occurred during the intervening years.

During the 1990s, the need for software developers to consider the social impacts of their work emerged. At the time software called Pretty Good Privacy (PGP), which offers anonymity and confidentiality for email was much discussed. In fact, the creator of PGP consulted Computer Professionals for Social Responsibility (CPSR) for an opinion before promoting the software. In response, CPSR gave its seal of approval saying PGP was very important to "computing freedom"<sup>i</sup>. PGP was then distributed over the Internet and has since become a de facto standard for ensuring the security and privacy of email communication. The creator of PGP was a researcher working on his own interests, an "amateur" programmer, and it is important to note that CPSR, a civil consulting body, functioned as a contact to discuss the possible impact brought by the software he had diligently created.

This anecdote is not intended to discourage developers from promoting potentially dangerous software. For example, a textbook written by Professor Ross Anderson of Cambridge University states the following: "The implication of all this for the security engineer is that

you have to think hard about the risk that your product or service will become the target of hysterical abuse by ineffective or corrupt public servants, or by ignorant and hypocritical self-publicists. You can't ignore the social and political context of what you're trying to build." <sup>ii</sup> In other words, Professor Anderson argues that computer development engineers should be ready to take risks and be prepared for attacks by third-rate bureaucrats.

So, how should we deal with the situation in Japan? The current "computer society" in Japan has only reached a stage comparable with that of the United States in the 1980s, and it is not possible to solve problems among experts alone. Even though academic society can pursue the latest academic developments, it does not have the ability to monitor people's opinions in the workplace nor respond to questions relating to the software created by amateur programmers. In an age when anyone can use P2P technologies, this issue needs to be addressed not only by academic societies but cooperatively across diverse organizations. I hope the League of Software Engineers (LSE) established based on FreeKaneko.com will play a role in these activities.

Next, we will discuss the mindset of software development engineers. Basically, development engineers chose

their profession because they enjoy it. The slogan "Just for Fun" is their starting point. Indeed, many engineers involved in development of Linux have said their motivation has been this "just for fun" philosophy. However, these days, engineers might get arrested for engaging in their activities "just for fun"! We need a philosophy that can withstand attacks from the outside, without damaging the spirit to pursue development "just for fun."

As mentioned earlier, the importance of software was discussed in relation to PGP from the viewpoint of ensuring constitutional values and civil freedoms. However, it sounds pretentious when we talk about constitutional values in Japan. It is therefore necessary to have a unique philosophy for software development engineers in Japan, and to conduct studies on what kind of values software empowers. We need to let the technologies speak for themselves to prove their real value, without making value-neutral excuses, saying that the problem is how the technology is used rather than the technology itself, nor referring to the Constitution. Here, the ethics of the hacker provide a clue.

Hackers are basically the type of people who program computers "just for fun." However, some of them demonstrate their philosophy through their works. For

example, there is a philosophical message embedded in internet technologies. The researcher who developed the World Wide Web initially developed and distributed the software to share copies of academic papers among researchers and papers published in academic journals were meant to be included from the outset. We can say that the World Wide Web reflects the culture of the research community globally that takes it for granted to distribute unauthorized copies of relevant academic papers. The developer might have been regarded as a "terrorist" in different times.

Cache technologies have also been considered harmful to the society because they helped to make illegal copies. However, the Internet Society (ISOC) and other internet engineers organizations have repeatedly insisted that a copy stored in cache is not an illegal copy. This effort has enabled cache technologies to be widely accepted and valued.

Technology is not neutral and values are embedded in it. I think it was the Kyoto Prefecture Police who seriously thought about this point in Japan yet misunderstood software as an anti-social philosophy! It can even be said that hackers uphold the philosophy of not concerning any philosophy. Stallman emphasized that open-source software must be "free." One aspect of this is the

freedom to execute a computer programme without questioning its purpose. According to Stallman, programs that "should not be used for criminal activity" are not free. Incidentally, in a document entitled "What Peer-to-Peer Development Engineers Should Know," the Electronic Frontier Foundation (EFF) has also stressed the importance of not attaching any prohibitions on software simply because someone might abuse it.

When Japanese people hear about the hackers' philosophy they tend to misunderstand it. But I believe hackers who have been successful in Japan give us clues that help us understand the culture of software originating from Japan. It reminds me of the film, "Densha Otoko (the Train Man)."

Winnie and the Train Man share an historic background, and bear some resemblance when we see them as phenomena. I would like to suggest that discussions about the emergence of Winnie could be even more significant than Train Man, despite the fact that the film has been widely spoken about. Never before has a software engineer organized a community of one million people, even crossing national boundaries. Only Winnie and Mr. Kaneko have accomplished this. Perhaps we need to convey to the world discussions

concerning Winny, and this could enable us to contemplate the new software

culture originating in Japan.

---

i The story of PGP's development and release is described in Simson Garfinkel, "PGP: Pretty Good Privacy". O'Reilly & Associates, 1994.

ii Ross J. Anderson, "Security Engineering: A Guide to Building Dependable Distributed Systems". John Wiley & Sons, 2001, 1st edition. Available on line:  
<http://www.cl.cam.ac.uk/~rja14/book.html>  
See Section 21.2.5