Surfing with Good and Evil

Jeffrey Barlow
Pacific University

Recommended Citation

This Editorial is brought to you for free and open access by the Interface: The Journal of Education, Community and Values at CommonKnowledge. It has been accepted for inclusion in Volume 4 (2004) by an authorized administrator of CommonKnowledge. For more information, please contact CommonKnowledge@pacificu.edu.
Surfing with Good and Evil

Rights
Terms of use for work posted in CommonKnowledge.

This editorial is available at CommonKnowledge: https://commons.pacificu.edu/inter04/20
Surfing with Good and Evil

Posted on April 1, 2004 by Editor

By Jeffrey Barlow <barlowj@pacificu.edu>
Editor, Interface

Introduction:

The last year or so has been one of tumultuous change in attitudes toward the Internet. The earlier period was one of relative optimism in which the Internet heralded progress in democracy, in commerce, in communications, and in the building of communities. Now the focus seem to be upon cyberstalkers, music and film piracy, spam, and a proliferation of frauds that is beyond comprehension, including Cyberjacking, a crime discussed below.

The Saints Preserve Us:

Catholics, properly concerned with the rapidly declining moral stature of the precincts of the Internet, are currently engaged in selecting an appropriate Saint to guard over it. [1] We wish the Catholic community godspeed in their search; the Internet cannot have too many mystical protections. But we nominate a figure from an earlier religion: Janus.

Janus has a lot going for him/her image-wise. Classically, the two-headed Roman god has guarded gates and doorways. Welcome pages, portals, even web browsers and email applications, would seem not to be much of a challenge. Janus also is often presented as being simultaneously male and female, deftly avoiding gender prejudice of any sort. [2]

It is true that Janus is definitely pagan, but this would not be the first such deity to be co-opted into modern religious ranks. Being pagan, Christians, Buddhists, Moslems and Jews should all be able to put their own sectarian spin on the process of enrolling Janus.

It may be, however, that Janus is too singular in the sense that while he/she looks backward and forward, there seems to be no classical reference of another split, one between good and evil. For divine beings who are appropriately dualistic we will probably have to seek farther afield, perhaps in Asian or Indian belief systems, and this is, let’s face it, just never going to be
acceptable as an image in the current Euro-centric incarnation of the Internet.

**Good and Evil:**

But whatever spirit we ultimately select, we are going to have to face the fact that it must represent the two poles of human behavior, good and evil. To a liberal, mankind is born innocent and corrupted by society; human impulses are good and can be trusted. To the conservative mind, mankind is more animal than anything else, and must be confined by law, religion, and custom to act properly.

Lately at Berglund, we have seen more of the latter than of the former. As much as we believe that the Internet could be a tool for human liberation, freeing the best impulses of men and women to build democratic communities, the Internet that we increasingly see does not seem to come from heaven. Our email is filled with spam driven by the worst impulses for profit, and seeking in many cases to fulfill the worse impulses of individuals to consume and to dominate.

We have just had our personal credit card endangered for the second time.[3] On the previous occasion, we are still not quite sure what happened but presume it was hacked out of a merchant’s database. On this occasion, it would seem that it was taken when a thief stole a merchant’s computer, including records of one of my transactions. This time, it was disarmingly easy to find the cause; the event is now so common that it is no longer a big deal. In fact, the very bank that surely should worry about my own confidence in its records, is now offering me insurance against identity theft!

**Cyberjacked:**

Over the last several months we also were an innocent bystander in another internet click-by crime. We were “cyberjacked”! This is one of the plethora of new Internet-related crimes that are often so complex as to be very difficult to describe. The purpose of the cyberjacker is to draw attention to his or her own materials or own site. Sometimes this is out of a desire to make a statement, other times a desire to profit. In this case, an individual was, for reasons unclear to us, furious with a given firm. The individual then copied a press release from this firm and placed in on the Internet, so that searches for that firm would turn up these sites. The press release was then followed by a carefully crafted attack on the firm and its service, capped with a link to another site presenting the individuals case in more detail, and with considerably more rancor.

This individual was truly angry, because he or she placed the notice on thousands of sites around the Internet. We fell victim because we operate as part of our teaching mission, a number of Bulletin Boards (BBS) where students discuss class assignments, etc. We leave these sites up for years in some cases, and leave them accessible to the public because they are often of wide interest. In this case, a site discussing issues relating to Vietnam veterans (one with many links to it on the World Wide Web), was cyberjacked—the miscreant simply posted into it.
When the targeted firm learned of the proliferation of accusations they began doing their own searches to find references to their firm across the net. Having identified such, including ours, they begin sending email to all sites where the messages had been posted. We have attached the targeted firm’s email to us to this editorial. [4] We will leave it to our audience to decide if this may be said to have been threatening. Certainly it caused no small amount of consternation here.

Ultimately we had to take down the entire BBS because we had no simple way of pruning it of the offending messages. This was a site with considerable traffic because many veterans’ groups had linked to it. Moreover, the incident raises critical issues for our other sites. Do we now require that our BBS be accessible only with a password given to our students alone? If so, we have now been cut off from a larger audience.

And the attempt on the part of the firm involved to cleanse the web is bound to fail. Our own search on similar postings turned up many thousands of them. And while the people in charge of the search and destroy operation at the targeted firm were polite and helpful when I called them, they continued to send me similar emails for several days after we had shut down our site, each increasingly serious in its tone. Even if all victims were as accommodating as we have been, it is easy to see that one compulsive mind working a few hours a day can easily stay ahead of several full-time employees (and very expensive ones as they require specialized knowledge in both electronic communication and the law) fully dedicated to contacting victims to force removal of offending materials.

Some may take a far more libertarian attitude than we did, and simply refuse to close down their sites over one posting. The legal issues are impossibly complicated because this case crossed at least three national boundaries of which we are aware: the United States, Canada, and Mexico.

It is unlikely that any series of lawsuits can possibly protect the firm against this sort of activity. The fact is simply that the Internet has monstrously magnified the ability of individuals to wreak this sort of harm, and unleashed a degree of creativity that legal systems may never be able to control.

We have, of course, no brief for the miscreant. Whatever the degree of their moral or legal justifications, cyberjacking our site was not among them. Such cyberjackings are most often even more harmful in that the miscreant places a sort of electronic cuckoo in the targeted site which most often carries the innocent surfer to a porn site. The posting on our site contained a simple executable program that should have automatically forwarded anyone who clicked on the message onto the final web site mentioned above. But, because we operate within something other than a Windows© environment, the macro program did not work.

**Conclusion**

Over the several years of publication of Interface we have been involved in a number of issues
relating to electronic security, the larger issue addressed here, and are working on still other reports to be released when we have completed our research. This work has been well received.

We have heard from grateful readers who felt that we had saved them from becoming a victim in frauds which we clarified in time for them to save their endangered resources. We have heard from author of books we reviewed, thanking us for our clear explication of the problems we all face. And given that we ourselves continually fall victim to credit card loss, identity theft, and now, cyberjacking, we are unlikely to be able to stop discussing this issue anytime soon. [5]

Our work has become so complicated that we finally began to worry about our own security, and have cooperated with a firm, Primedius.com [6], to better protect ourselves electronically. Primedius is now listed as a supporter of the Berglund Center because they provide software, facilities and timely advise to help us in security-related issues. There are several such firms on the Internet, but we have found that Primedius has provided us with a degree of protection that we earlier lacked, and a much greater sense of security. But when all possible protections are taken, we think that Good and Evil will remain the hallmarks of the Internet. We may as well get used to it, while upgrading our own knowledge and protective wards, electronic or spiritual as they may be.

Notes:

Accessed 3/22/04.

[2] For a page of images see:
Accessed 3/22/04.

http://bcis.pacificu.edu/journal/2003/04/edit.php
and “Financial Transactions on the Internet, Part II”,
http://bcis.pacificu.edu/journal/2003/05/edit.php


[5] It seems appropriate to add that our victimizations are not caused by the fact that we are either cyberaccident prone, or particularly stupid, but largely a result of the fact that we have so many links to our sites out on the Internet. When spammers and others collect addresses they do so by sending ‘bots, spiders, or siphons (all terms for a sort of program) out on the Internet to
“harvest” email addresses. As our traffic is collectively well over 5 million pages served per year, and many of those have my email address on them, it is passed through many unsavory hands.


This entry was posted in Uncategorized by Editor. Bookmark the permalink [http://bcis.pacificu.edu/interface/?p=2941].