From: Ted Byfield <byfieldt@newschool.edu>
Subject: policy report
Date: June 19, 2010 12:39:55 PM EDT
To: XXXX
Cc: XXXX, XXXX

Hi, XXXX, XXXX, XXXX --

I've attached my report on the new Safe•Connect ("SC"), made by Impulse Point LLC ("IPLLC"), the new authentication system required for wireless access. It's long (20 pages), dense (~50 footnotes), and often very technical. I apologize in advance for that, but I know of no other way to cover so much material -- software design, protocol analysis, legal issues, corporate histories -- in the necessary level of detail.

SC was initially developed to function as music-related spyware, and it still has this capability.

* IPLLC previously stated that SC can scan, analyze, report, index, and even remotely destroy music files.

* IPLLC currently states that SC can scan, analyze, index, and report music files.

* IPLLC has used its SC network to compile a centralized "library" of "fingerprinted" music files.

* IPLLC consistently cites the RIAA (Recording Industry Association of America) as a legal authority, but has never mentioned FERPA or any education-related privacy legislation.

* IPLLC's privacy statement states that third-party websites "accessed in conjunction with the Impulse Safe•Connect NAC System are not covered" by the policy.

* The SC software agent directly connects to what looks like a third-party site but in fact is operated by another legal entity with the same corporate officers at the same street address.

IPLLC stresses that host institutions such as NSU can configure specific "policies" (regarding antivirus software, spyware, and so on). However, the overall system architecture -- from the design of the software agent that users install, to the IPLLC's IT infrastructure, to IPLLC's and its related companies' corporate structure -- may allow IPLLC et al. to circumvent these policies and collect information autonomously. There is a serious risk that its use constitutes a systematic violation of FERPA.

However, the risk of FERPA violations is only emblematic of the broader issue posed by NSU's adoption of SC. It is a dramatic assertion and expansion of authority by NSU: in exchange for transient access to NSU's

wireless network, users are required to install software that continuously surveils every user of a computer -- friends, colleagues, family, children -- without regard to who owns the computer. Given NSU's progressive mission, it is entirely reasonable to assume that this policy may directly conflict with the beliefs of many of the affected people, may contravene policies and practices of organizations they are affiliated with, and/or may violate other laws to which they are subject.

I believe that SC is incompatible with NSU's history, values, and mission -- and I'm certainly not alone in this regard. If the history, capabilities, and operations of SC were plainly stated when users are asked to install it, many NSU stakeholders would refuse it. And if the system had been submitted for approval by academic governing bodies prior to implementation, it almost certainly would have been roundly rejected. Thus, SC poses a very serious reputational risk to NSU. This is particularly pressing, given that it applies to ACT/UAW members, guests of NSU-sponsored events such as the recent "Limiting Knowledge in a Democracy" and "Games for Change" conferences, and visitors from other academic institutions.

I am submitting this document to you with the request that you will promptly initiate an appropriate process for reevaluating NSU's adoption of SC. My own recommendation is that it be suspended immediately, pending further review.

However, I want to stress that the questions I have posed here are not limited to NSU. SC has been adopted by dozens of higher-ed institutions around the country and affects hundreds of thousands of people. Consequently, it presents a serious public-interest problem. My analysis is very detailed, but it is just the work of one person, so I intend to work with peers at other academic and advocacy organizations for further analysis and action. Thus, time is of the essence in this matter. In less than three months, the academic year will begin -- everywhere, not just at NSU.

Thanks for your time and attention, and I look forward to your response.

Cheers,
Ted

19 June 2010

Dear Tim —

I'm writing to express my concerns about the NSU's new wireless access policy. I have consulted with a number of NSU faculty and staff members in defining these concerns and drafting this letter. The informal consensus is that the new system is extremely troubling.

NSU's IT staff no doubt adopted the new system in a good-faith effort to maintain an effective wireless network infrastructure and to implement much-requested new services (e.g., wireless printing). However, this new system and its implications extend far beyond NSU's wireless networks. It affects computers that are not owned by NSU and people who have no affiliation with NSU, and it raises serious questions about what information this system discloses, to whom, and to what end. ***It's reasonable to ask whether the potential ethical, legal, and reputational risks of this system outweigh the limited benefits that NSU IT has offered as justification for adopting it.***

Previously, wireless access required a simple web-based authentication system (i.e., a login with a valid NSU username and password). In contrast, the new system requires the installation of an application called "Safe•Connect". Under the new system

1. installation of the Safe•Connect "agent" (sometimes called the "Safe•Connect Policy Key") is required for anyone who accesses NSU's wireless networks, regardless of who owns the computer or the nature of his or her affiliation with NSU. So, for example, guests of the NSU who need temporary wireless access (for example, at a conference) are required to install the agent.

2. Once installed, Safe•Connect launches itself automatically, runs at a system level (i.e., when a computer boots, not when a particular user logs in), runs continuously, runs with "root" privileges, and when terminated immediately relaunches itself. As a result, it is imposed on all users of the computer (spouses and partners, children, friends, and colleagues) all the time.

It is reasonable to ask whether it is in NSU's interests to establish a policy under which transient access to its wireless network is made conditional on the installation of an invasive application.

After a browser-based authentication system (like NSU's previous system) grants a computer access to a network, most of the computer's activities remain a 'black box.' An enterprise-level network infrastructure should be able to analyze its external behavior — for example, which numbered ports are open and how much inbound and outbound traffic is passing through them. Because many ports are assigned to particular functions (e.g., port 80 for web [HTTP] traffic), it is often easy to tell in a generic way what kinds of applications are running on a networked computer. Similarly, it is trivial to prevent unwanted activity (e.g., peer-to-peer or "P2P" applications) by blocking certain ports — as NSU has done for years.

However, Safe•Connect installs an application that has unlimited privileges and can communicate independently. It can provide unfettered access to the computer's resources and workings in real time —

the ability to see any and every process and application running, to inspect file structures, to read and write files, and so on. Thus, the introduction of Safe•Connect at NSU isn't just a new login procedure; instead, *it dramatically expands the NSU's ability to surveil and regulate the activities of any and every computer that, however fleetingly or occasionally, has connected to NSU's wireless network.*

Safe•Connect's manufacturer, Impulse Point LLC of Lakeland, Florida (hereafter "Impulse Point"), emphasizes that a host institution can define whichever computing 'policies' they want to enforce (for example, network configuration, antivirus software, file "sharing," etc.). So, one could argue, it doesn't really matter what Safe•Connect 'could' do in the abstract, because NSU has implemented the system in a minimal way. However, the issues at stake are *not* reducible to merely specific questions about its technical implementation. To argue otherwise would be tantamount to arguing that the academic institution itself and its operations are exempt from academic inquiry — which is antithetical to the vision that has driven many positive changes at NSU in recent years.

But let me offer you a concrete example. My research has led me to conclude that the Safe•Connect system served as a spyware network and very possibly still does so; on point of principle, then, I will not install the software on my computer. Setting aside the ongoing burden this will entail, which is a consequence of *my own choice,* what should I do when I see colleagues and students using it? Should I say nothing, lest I cast doubt on NSU and risk causing problems that would ramify across other settings (e.g., classes) where use of the wireless network is assumed? How should I respond when guests install it, given that I know full well that it will likely run indefinitely on their own computers? Or — as seems *right* in a progressive educational institution — should I speak out on the basis of my knowledge and beliefs? This dilemma is certainly sharpened by my deeply held beliefs about how our cultural heritage and society are being distorted by maximalist claims about "intellectual property"; but it is is a *dilemma* because the choice — either accept a system I believe to be malicious or forgo NSU wireless access — is an artificial and inappropriate quid pro quo. However, the following discussion isn't about abstract principles; if anything, it's far too technical.

I'm fairly sure that if Safe•Connect's history and full range of capabilities were plainly stated when users are 'asked' to install it, very few people would agree to do so. But this information isn't disclosed, so from the outset there is a risk that many people might feel that Safe•Connect is presented ways that are at least incomplete and possibly misleading.[1] However, once someone has installed it, if s/he objects, his or her only option is to uninstall the Safe•Connect agent —which is an extremely obscure process. I haven't looked at the Windows version of the application, but on a Mac it requires specialized knowledge of how to manipulate the internal resources of an application. Many installers or "package" (.pkg) files include an explicit uninstall option in their interface or in a documentation file (e.g., a "Readme"). Safe•Connect's does not; nor does it make any reference to how or why one might want to do so — for example, to

---

[1] Williams College has taken an unusually candid approach. Their documentation (which I believe is distinct from the installation interaction) states that "[t]he Impulse system has the ability to enforce policies forbidding the use of Peer2Peer filesharing applications. It also has the ability to require a user to log in every time they attach to the network. **Those features will not be turned on.** Williams' policy does not currently forbid the use of any specific software. We require people to log in when they register their computer on the network for the first time and feel that is enough" (emphasis in the original). [http://wiki.williams.edu/display/docs/Impulse]

minimize the unreasonable amount of memory it consumes.[2] It is very unlikely that anyone lacking technical knowledge and confidence would do this; and, based on my conversations with colleagues at NSU, even technically sophisticated users who have removed it are skeptical that it is really gone. ***Thus, it seem reasonable to conclude that, once installed, Safe•Connect will run in effect "forever" — that is, until the computer is overhauled or replaced.***

Impulse Point is demonstrably aware of this, which suggests that this obscurity may be by design. For example, the "SCUninstall.app" embedded within the agent invokes an uninstaller script ("Uninstall.sh") which itself states:

> `This script must be run as root. It took root privileges to install this product, it will take root privileges to uninstall it.`

Moreover, the same file includes the following comment regarding the preferences file that the Safe•Connect agent installs:

> `I am unsure if /Library/Preferences/loginwindow.plist is only being used by us. It has not been deleted for this reason. If it was only used by us, then it will continue to try and launch a program that isn't there each time a user logs on. This should not hurt anything, but may appear in error log reports. You may wish to inspect it and remove it yourself if you are so inclined.`

This shows that Impulse Point knows that Safe•Connect might conflict with other applications or services.[3] Indeed, in programming for the Mac OS it is standard practice for a preferences file of this kind to include the vendor's name (e.g., "com.impulse.loginwindow.plist") precisely in order to avoid such confusion and to facilitate troubleshooting. Rather than openly disclosing the file's origin, Safe•Connect violates standard practice by using a generic "system"-sounding filename to launch the Safe•Connect agent.

This letter isn't the place to offer a detailed critique of Impulse Point's approach to programming, but I will note in passing that a perfectly normal approach would be a discretionary application (for example, installed on the Desktop and called something clear like "New School Wireless Connect") that a user would launch when s/he wants to connect to NSU's wireless network and could quit when s/he wanted to log off. The facts that Impulse Point (1) installs a faceless, root, always-on application, (2) provides no documentation about how to uninstall it, and (3) knowingly invites and then dismiss the resulting risks by obscuring key files are all noteworthy. NSU IT cannot be expected to answer questions why Impulse Point would choose such an opaque and heavy-handed approach. ***However, it is reasonable to ask whether such a system is in the best interests of NSU and its constituents.***

---

[2] In order to remove the Mac version, a user must: (1) find the Safe•Connect agent application, (2) right-click on it, (3) select "Show Package Contents" from a contextual menu with many items, (4) navigate through a file structure to find the "SCUninstall.app", (5) extract it, and (6) run it with "root" privileges.

[3] I have also heard anecdotal reports that it interferes with connections to some non-NSU wireless networks.

According to NSU IT's "Privacy, Security, and the Safe•Connect Policy Key" webpage,[4]

> *The Safe•Connect agent is designed to determine the true or false status of very specific computer states. The university uses it to determine the following:*
>
> - *Is an anti-virus program, installed, running and have updated virus definitions? (Windows)*
> - *Is the computer getting its IP address via DHCP from a New School DHCP source? (Windows/Mac)*
> - *Is the computer configured to use an approved DNS server? (Windows/Mac)*
> - *Is the computer configured to use a New School defined network gateway? (Windows/Mac)*

These questions are both sensible and legitimate. However, NSU IT's "Wireless" webpage[5] acknowledges the following:

> *Q: Does newschoolnet check for Anti-Virus updates for Mac, Linux, etc?*
>
> *A: No. There are no checks for operating systems other than Windows. The Windows OS is most susceptible to Viruses, Spyware, and other risks.*

Thus, the stated benefit of requiring the use of Safe•Connect for Macs and other portables (I omit Wifi-enabled mobile phones [iPhone, Android, high-end Nokia, etc.]) boils down to getting very basic network information — all of which could be gathered and/or enforced by other, less intrusive means.[6] ***Given the prevalence of non-Windows-based portables at NSU, it's reasonable to ask whether Safe•Connect's PC-oriented benefits outweigh its drawbacks for computer users as a whole.***

The same webpage states that

> *The Safe•Connect agent is in use at many universities around the country, including Oberlin College, Yeshiva University and the Albert Einstein School of Medicine, University of Rhode Island, Bucknell University, UCLA, and Syracuse University.*

Of course, the fact that a handful of higher-ed institutions have adopted this system carries much less weight than the *thousands* of institutions that require nothing of the sort and, instead, rely on the de facto global standard of web-based authentication. ***Thus, it's reasonable to ask what peculiar***

---

[4] http://www.newschool.edu/at/network/wireless/privacy_security_SafeConnect.html

[5] http://www.newschool.edu/at/network/wireless/index.html

[6] A search of NSU's website for "DNS" currently returns zero hits, so how are users to know what "an approved DNS server" is?

circumstances NSU faces that — to name just a few neighboring institutions —City College, Columbia, Fordham, Hunter, NYU, and Rockefeller do not.[7]

From one institution to the next, there's a striking similarity to the language with which IT departments describe Safe•Connect — because much of that language is adapted, with minor changes, from Impulse Point's own boilerplate.[8] Nevertheless, these 'variations on a theme' provide an interesting window into the various strategies that different institutions use to make the Safe•Connect system seem acceptable to their users. A thorough analysis of these rhetorical strategies would, I assure you, be tedious, so I'll just summarize the main ones:

- *emphasize the benefits;*
- *fiat statements* (e.g., "The Policy Key is not spyware"[9]);
- *overly specific language* (e.g., "The policy key strictly collects policy status information which is required for the operation of the Impulse Safe•Connect NAC System"[10]);
- *red herrings* ("it cannot monitor your e-mail, web, IM, or other internet traffic"[11]); and
- *escape clauses* ("The policy key only checks specific security requirements; or perform any other function that would interfere with *your legitimate personal computing privacy*."[12])

One problem that arises when IT staff 'outsource' substantive policy communications (which in this context are conflated with technical documentation) to a vendor like Impulse Point is that the result is utterly disengaged from its educational context. Its tone might strike some as dictatorial rather than persuasive; and if it includes statements that might be seen as evasive, misleading, and/or obfuscating, it directly undermines both the form and substance of the institution's educational mission. What could have been a "teachable moment" of the best kind — a concrete, ethical choice in a shared context, in this case of a school's network — becomes the opposite. ***It's reasonable to ask whether there is any other context in a higher-ed institution in which this approach would be acceptable.***

---

[7] Columbia and NYU, and perhaps more, maintain open wireless networks; and several institutions require Safe•Connect *only* for Windows-based PCs — demonstrating that such a configuration is possible.

[8] For example: *Impulse:* "The Policy Key is a lightweight software application that ensures the end user is in compliance with an organization's access policies" [http://www.impulse.com/solutions.php]. *NSU:* "The Safe•Connect Policy Key is a lightweight software application that must be installed on both Windows and Macintosh computers in order to connect to the New School's wireless network. The Safe•Connect agent is used to ensure that any computer accessing this network is in compliance with The New School's Information Security policy" [http://www.newschool.edu/at/network/wireless/privacy_security_SafeConnect.html]. *And so on.*

[9] http://map.ais.ucla.edu/portal/site/UCLA/menuitem.789d0eb6c76e7ef0d66b02ddf848344a/?vgnextoid=a02662677f17f010VgnVCM100000db6643a4RCRD

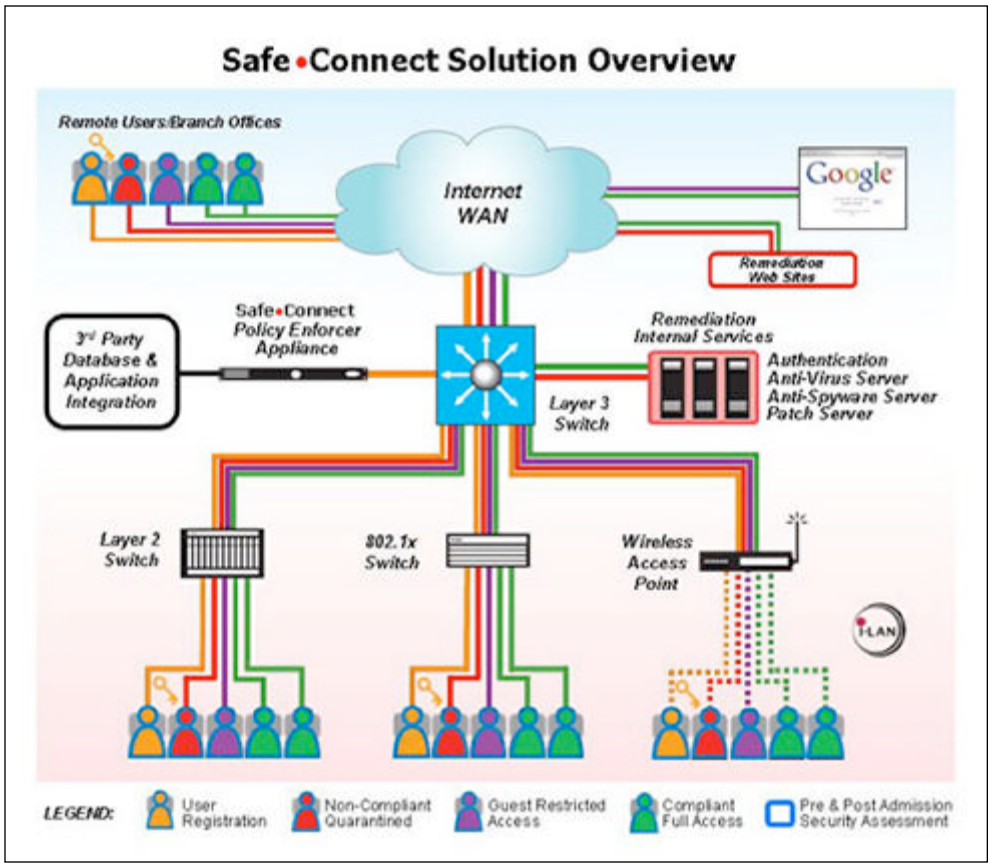
[10] http://resnet.nau.edu/Docs/Impulse-Privacy-Statement.pdf

[11] http://helpdesk.owu.edu/NWSecurity

[12] http://helpdesk.owu.edu/Impulse

This lack of clarity is unfortunately evident in NSU IT's explanation, which states that "[t]he Safe•Connect agent is designed to determine the true or false status of very specific computer states," and then lists what exactly "[t]he university uses it to determine." This explicit list is helpful, to be sure; but the explanation sidesteps acknowledging that the agent is just one part of a large Safe•Connect system, and that in the Safe•Connect system can in fact examine, report, and log many other things — in particular, certain kinds of applications and files.

Impulse Point's own diagram (which is incomplete in ways that are central to this analysis) shows that another essential component is a server called the "Safe•Connect Policy Enforcer Appliance," which is installed within an institution's network infrastructure:[13]



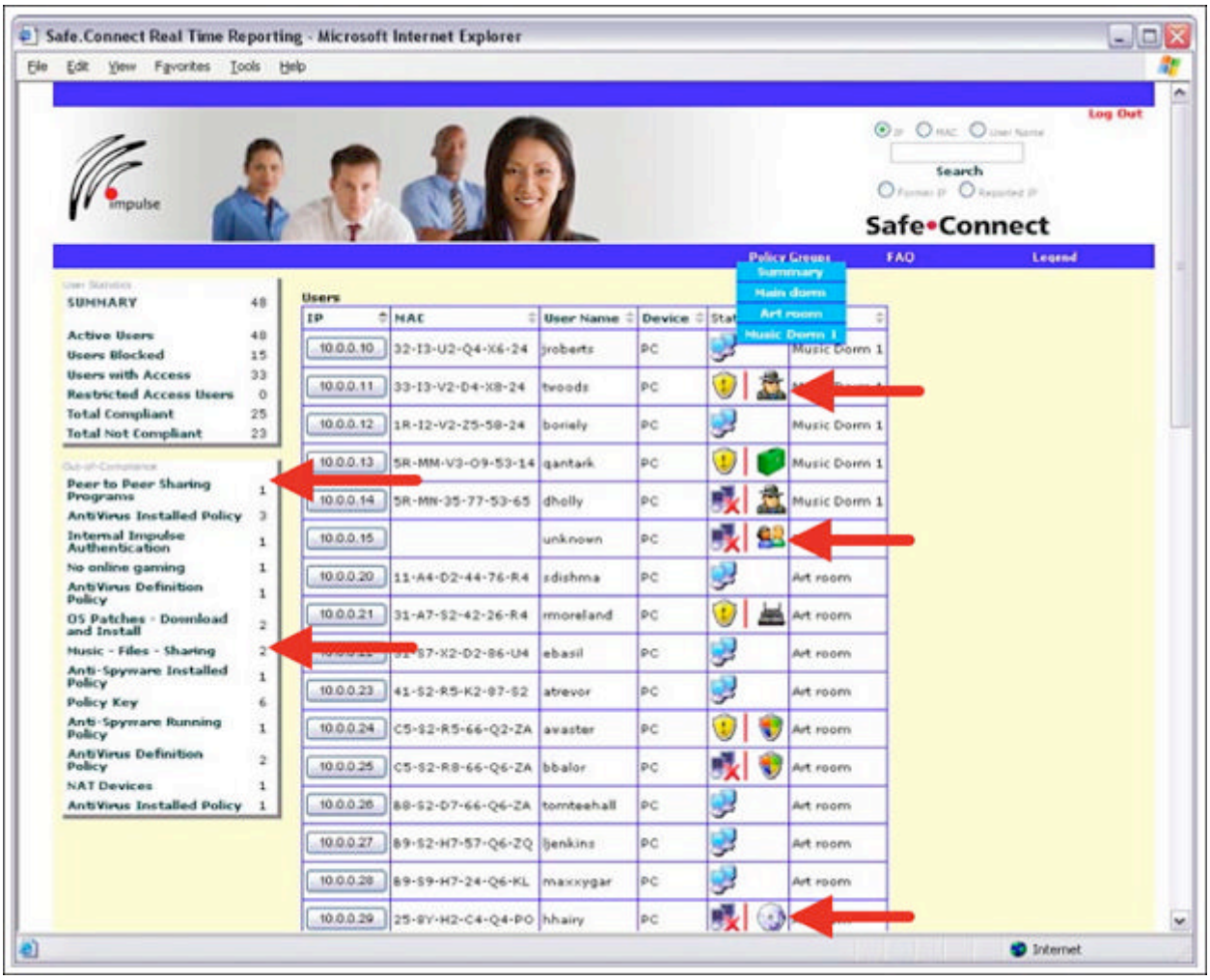
In Impulse Point's "Regulatory Compliance and NAC White Paper"[14] a screenshot of the "Safe•Connect Policy Manager" web-based console shows that it aggregates institutional usernames (e.g., an NSU NetID), MAC addresses (i.e., the unique serial number of a computer's network interface), IP addresses, *as well as applications and files*. These are represented with icons: a cartoonish 'spy,' presumably for spyware; a 'CD,' presumably for (as the left column states) "Music - Files - Sharing", two "friends"

---

[13] http://www.impulse.com/solutions.php Note, however, that this diagram is incomplete because it omits Impulse Point's own in-house data center.

[14] http://www.impulse.com/downloads/Regulatory_Compliance_&%20_NAC.pdf

presumably for “Peer to Peer Sharing Programs”, and so on (I have highlighted these elements with red arrows):



Impulse Point’s website offers numerous “case studies” that describe how “the Safe•Connect system records vital ***student*** and computer devices statistics such as host name, device type, operating system, and MAC address,” “automate[s] the process of ensuring that ***student*** computers [are] not configured as outbound file sharing servers,” “provides up-to-the-minute information on their authentication and policy compliance status,” “reports non-compliance to the Safe•Connect Policy Enforcer and delivers individualized remediation guidance,” and so on (emphasis added).[15] Another case study states that their system “delivers real-time and historical policy status reporting” — in other words, it keeps cumulative logs — “that provides valuable insight into group or individual policy compliance.”[16] Clearly, then,

---

[15] Variously, “How Do You Solve the Back-to-School Blues?” [http://www.impulse.com/downloads/solve_back_to_school_blues_reduce_costs.pdf] and “How Do You Stop the Music?” [http://www.impulse.com/downloads/stop_music_illegal_p2p.pdf].

[16] http://www.impulse.com/downloads/centralized_approach_k12_berkeley.pdf

according to Impulse Point's current promotional literature, the Safe•Connect system *as a whole* can and does report and log a wide range of information.

I do not know which features ("modules") NSU IT has implemented, but its "Privacy, Security, and the Safe•Connect Policy Key" webpage states:

> *The Safe•Connect agent is used to ensure that any computer accessing this network is in compliance with The New School's Information Security policy. The agent does not report or log any information other than what is required to ensure this compliance with university policies.*

What is "required to ensure this compliance with university policies"? Even a quick review of NSU's 21-page Information Security Policy makes clear that this exception can be construed to include anything and everything — again, without clearly delineating computers that are owned by NSU from those that are not.[17] NSU's "User Responsibilities" statement ("Revised June 18th, 2008") similarly affirms this when it states:

> *All users are reminded that there is no right to privacy with regard to the University's computing and network resources and user accounts may be accessed by the University at any and all times. The University reserves the right to limit, restrict or extend computing privileges and access to its resources. University resources include all computing and network resources operated by the New School or purchased or leased from an external entity for use by the New School.*[18]

Thus, Impulse Point punts on all privacy issues to host institutions; and, in the case of NSU, there is no right to privacy" — which extends to "computing and network resources [...] purchased or leased from an external entity for use by the New School" — which would seem to include Impulse Point.

One of the curious features of Impulse Point's promotional literature is the inconsistency with which it addresses fundamental higher-ed concerns. For example, the summary 'pitch' stated in thirteen out of sixteen case-study PDFs on their site[19] claims that the Safe•Connect system was primarily "designed for higher education's unique environment." If so, then it's noteworthy that the litany of regulatory frameworks cited in their "Regulatory Compliance and Network Access Control (NAC)" document — "Sarbanes-Oxley, HIPAA, Basel II, and Graham-Leach-Bliley, to SEC Rules 6835 & 17-a, TREAD Act, FCC-LSOG, USA Patriot Act, CALEA, PCI Security Scans, and the California Security Breach Notice Law" — doesn't mention FERPA (the Family Educational Rights and Privacy Act).

---

[17] http://www.newschool.edu/forms/Information_Security_Policy_New_School.pdf . NSU's Information Security Policy (June 2007) appears to be substantially 'based on' Georgetown University's (May 13, 2003), less the GU document's discussions of privacy, an Acceptable Use Policy, and periodic review.

[18] http://www.newschool.edu/at/policies/resp.html

[19] http://www.impulse.com/literature.php

FERPA would seem to be especially relevant given that Impulse Point specifically names "students" as the focus of Safe•Connect's monitoring. Yet there does not seem to be a single mention of FERPA anywhere on Impulse Point's current website; nor have I found any mention of it in any archived version of their website going back to December 13, 2003.[20] Given the range of the other legal frameworks cited — which are heavily weighted toward financial entities and publicly held corporations — this omission is astonishing. Moreover, the only discussion of privacy issues at all on Impulse Point's website is the privacy policy pertaining to the use of their website itself, which includes a peculiar mention of COPPA, the Children's Online Privacy Protection Act of 1998[21] — hardly relevant to "higher education's unique environment."

One could argue that the basic information that the Safe•Connect system *must* process for authentication (NetID and password) falls squarely under FERPA's "directory information" exemption (which is typically construed as covering name, address, phone number, email address, DOB, and so on for the purposes of class rings, yearbooks, and the like[22]). However, this argument has two key weaknesses. First, however confident Impulse Point may be that their system is covered under this exemption, it hardly follows that every potential client would share their confidence to such a degree that the issue needn't ever be broached. And, second, if Impulse Point's legal understanding of the subject is so consummate, why would they cite as relevant the Transportation Recall Enhancement, Accountability and Documentation Act of 2000, which was enacted "to require a warning system in new motor vehicles to indicate to the operator when a tire is significantly under inflated"?[23]

Occam's Razor suggests a more economical explanation for why Impulse Point hasn't mentioned FERPA: they don't think it pertains to them. ***If so, it's reasonable to ask whether it's prudent for NSU to require users to install software from a vendor that, since its founding in 2004,[24] has shown no interest in federal privacy requirements for educational institutions.***

The Internet Archive (archive.org) is a nonprofit digital library that "offers permanent storage and access to collections of digitized materials, including websites, music, moving images, and books." Toward that end, it's "Wayback Machine" crawls large segments of the web in order to take periodic 'snapshots.' The snapshot of Impulse Point's website as of 9 June 2005 states that the Safe•Connect system's "music module"[25]

> *will scan the end-user machine for music files as well as monitor all music files which are added to the computer. Depending on the policies set by the client, it can stop any downloads or sharing of illegal music files and make any already downloaded illegal files*

---

[20] http://web.archive.org/web/*/http://www.impulse.com

[21] http://impulse.com/privacy.php

[22] http://www2.ed.gov/policy/gen/guid/fpco/ferpa/mndirectoryinfo.html

[23] http://www.nhtsa.gov/nhtsa/announce/testimony/tread.html

[24] http://www.corporationwiki.com/Florida/Lakeland/impulse-point-llc-5978924.aspx

[25] http://web.archive.org/web/20050210224328/www.impulse.com/index.php?id=modulemusic

> *unplayable. Implementation of this module will enable the client to address legal concerns of the RIAA [Recording Industry Association of America, i.e., a trust that lobbies for the music industry] and the associated piracy and property theft issues.*

Thus, according to Impulse Point itself, the Safe•Connect *agent* was specifically designed to rummage through a user's hard drive, report detailed lists of files, facilitate analysis of those lists over time, and, if remotely directed to do so, *destroy those files.* ***It's reasonable to ask whether the members of the NSU' community should allow software with capabilities like this to be installed on their computers.***

Two bulleted feature lists on the same webpage describe the system's functions and include:

> • *Block Song Editor (by name, ICD code)* — which assumes that Impulse Point possesses a purportedly authoritative list of music files (ICD codes), against which it compares the files that the Safe•Connect agent finds on a hard drive; and
>
> • *Select IP range/subnets/domain to include/exclude* — which assumes that the Safe•Connect agent is in fact capable of analyzing information about websites (i.e., domains) visited by a person.

Another bulleted list on the same webpage describes "Managed Service provided by Impulse Data Center" — that is, IT services provided not by the Safe•Connect "Policy Enforcer Appliance" installed within an institution's (e.g. NSU's) network but, instead, by Impulse Point at its own data center in Lakeland, Florida.[26] These functions are:

> • *Maintain music library*
> • *Update Block Song List*
> • *Maintain Fingerprint Library*
> • *Maintain Fulfillment links*
> • *Maintain Advertiser library*

This strongly suggests that Impulse Point's business model circa 2005 was to develop a distributed architecture to surveil computers for music files, "fingerprint" them (conventional shorthand for generating a cryptographic string of characters or "hash" unique to a particular file), and aggregate the resulting information — and very possibly personally identifiable information as well — to a centralized database at Impulse Point's data center.[27]

---

[26] http://www.dsm.net/dsm/datacenter.aspx

[27] Impulse Point's "managed" services can be extensive. Some schools (e.g., Troy University [https://it.troy.edu/networking/nac.html], of Troy, Alabama], Canadian University College [http://old.cauc.ca/MainPages/CampusServices/ComputerServices/faq.html], and the College of New Jersey [http://userscripts.org/scripts/review/69331]) require users to log out *by connecting directly to a webpage hosted on Impulse Point's webserver* at http://auth.impulse.com:8008/html/logout.htm . In these cases, Impulse Point has direct access to users' login IDs and passwords, and therefore unfettered access to users accounts. There can be little doubt that such an architecture has implications for the purposes of FERPA.

Where Impulse Point obtained this purportedly authoritative list of music files is an interesting question, to say the least. The obvious candidates are (a) through its own data collection via Safe•Connect installations, and/or (b) the RIAA and/or other music-industry sources. The mentions of "ICD codes," "fulfillment links," and an "advertiser library" hint at a more complex business model in which Impulse Point may have sought to exploit the data it aggregated into some sort of brokering or "affiliate" role between music distributors and consumers.[28] If so, then it's even more likely that Impulse Point has directly or indirectly provided information it gathered through Safe•Connect installations to representatives of the music industry (e.g., the RIAA[29]). The value of that information would likely increase dramatically if it included personally identifiable information — as a basis for 'approaching' institutions about alleged intellectual-property violations on their networks, for suing individuals (for which the RIAA is well-known), and/or for brokering music purchases.[30]

If Impulse Point's current promotional literature is taken at face value, something like this may still be their business model. According to their website, the Safe•Connect "p2p file sharing module [...] validates computer content for compliance with legal issues such as digital rights management and copyright infringement."[31] Validating "content" for "copyright infringement" would require that Impulse Point maintains a database that's purportedly able to discern 'infringing' from 'non-infringing' content, and that the Safe•Connect agent is capable of "fingerprinting" and "reporting" content on a user's computer.

Before proceeding further, it's reasonable to ask several questions:

---

[28] "ICD codes" is probably "intelligent content delivery" systems, a popular buzzword ca. 2006 for efforts to rationalize network traffic involving large media files and streams — often tied to subscription services.

[29] At the January 30, 2008, "State of the Net" conference [http://www.netcaucus.org/conference/2008/] hosted by the Advisory Committee to the Congressional Internet Caucus, RIAA President Cary Sherman said: *"Filters can be put in the applications, for example. You know, one could have a filter on the end user's computer.[...] Why would somebody put that on their machine? They wouldn't likely want to do that, but they'd do that when it benefits them such as for viruses and so on and so forth — that's the sort of thing that could be enforced at the modem or something that's put in by an ISP. So there are ways that it could be addressed... I don't think you should underestimate the educational benefit of these kinds of things."* [http://www.youtube.com/watch?v=dxYGZ7Z6joQ&feature=player_embedded#]

[30] One publicly available version of Impulse Point's "Safe•Connect Quick Start Guide" states, under the heading "Automated Backup and Restore," that

> The Safe•Connect Policy Manager's policies and settings, including all custom policies and web pages, are backed up to the Impulse Support Center every 24 hours via an automated process. The Customer's Policy Manager daily backups are securely stored in a repository at Impulse Point for a period of seven days.

It isn't at all surprising that Impulse Point would have access to its clients' policies, and indeed they explain the resulting benefits. However, this information could also give them, or any party with whom they share it, a direct understanding of how aggressively various institution are in "endorsing" or "promoting" intellectual-property interests. [http://www.calfrye.com/notworking/quickstart.htm#sec20]

[31] http://www.impulse.com/policy-modules.php#6

1. ***Does Impulse Point currently maintain a "music library," a "fingerprint library," and/or any functionally equivalent store of data?***
2. ***If not, when did they stop? Why did they stop? And, prior to stopping, with whom did they share it? Or,***
3. ***if so, where do they obtain this information? With whom do they share it?***
4. ***if so, did they fully disclose these activities to NSU?***
5. ***Is the Safe•Connect agent capable of "making any files unplayable"?***
6. ***If so, how does Safe•Connect determine which files to do this to?***
7. ***If not, when and why was the capability removed?***

These questions are far from exhaustive.

Impulse Point changed its marketing literature soon after June 2005 to make its claims more anodyne. It began to speak of "prevent[ing] the outbound sharing of illegal music content," "coach[ing] ethical behavior through positive promotion," and "refer[ring] the end user to legal on-line procurement alternatives." The previously noted "Music Module" disappeared between February 10 and November 20, 2005, and was replaced a "p2p file sharing module," which, according to Safe•Connect's current website,

> *enables the organization or school to* ***promote*** *the legal concerns of the Recording Industry of America (RIAA) and other copyright and music piracy organization's concerns.*[32] [emphasis added]

Interestingly, the current formulation is more partisan than the earlier, pre–June 2005 formulation in which the Safe•Connect system merely "enable[d] the client to *address* legal concerns of the RIAA and the associated piracy and property theft issues."

Thus, despite overhauling its promotional language, Impulse Point's advocacy for the RIAA and "other copyright" concerns, appears to remain unchanged to this day. ***It's reasonable to ask whether NSU should entrust access to sensitive information to a vendor that, from its inception, has consistently cited a profit-seeking industry trade and lobbying group rather than federal educational-privacy legislation as a relevant legal authority.***

While NSU is legally bound to comply with FERPA, that legislation hardly exhausts NSU's interests in safeguarding the privacy of its faculty, staff, students, guests, and — as noted — anyone else, affiliated or not, who shares a computer on which NSU's Safe•Connect agent has been installed. Thus, it makes sense to look beyond FERPA in examining the role the privacy plays in Impulse Point's literature.

As NSU IT notes, "many universities around the country" have adopted the system. I've found only three instances in which Impulse Point itself addressed Safe•Connect vis-à-vis privacy concerns: Oberlin College, Northern Arizona University, and Yeshiva University's Einstein College of Medicine.[33] In each

---

[32] http://www.impulse.com/policy-modules.php#6

[33] *Oberlin:* [http://citwiki.oberlin.edu/images/2/20/Impulse-Privacy-Statement.pdf]; *NAU:* [http://resnet.nau.edu/Docs/Impulse-Privacy-Statement.pdf]; *Einstein:* [http://www.einstein.yu.edu/ITS/Uploads/Impulse%20-%20Privacy%20Statement%20V2.pdf].

case it is the same "Safe•Connect Privacy Statement" PDF, down to the creator and timestamps preserved in the metadata.[34] Since the same document covers implementations that may differ at the outset and change over time, it presumably covers every possible implementation, from the most minimal to the most maximal. Thus, users at an institution with a minimal implementation should take no comfort from it: if the monitoring becomes more aggressive, the privacy statement will still be 'true.'

For such a short document (less than two pages), it draws a plethora of extremely unusual distinctions: "personal information" vs. "personal end user content information" vs. "personally identifiable information about the end user" vs. "direct personal information" vs. "information that can link it directly back to end user personal content." These raise more questions than they put to rest. *By my reading, the privacy statement allows the Safe•Connect system to perform the same functions that Impulse Point advertised before overhauling its literature, namely, "scan[ning] the end-user machine for music files as well as monitor all music files which are added to the computer," and so on.* ***It is reasonable to ask whether NSU's contract with Impulse Point unambiguously forbids Impulse Point to gather, analyze, and/or share this data or data like it 'directly' or 'indirectly.'***

Moreover, as I noted earlier about descriptions of the Safe•Connect system, the document makes very specific claims about particular components in the Safe•Connect system (the "Policy Key" and "Policy Enforcer Appliance") *but omits mention of the managed services component.* In doing so, it may convey a misleading sense of completeness. Based on the document's organization, where one would expect it to mention these services, it says the following:

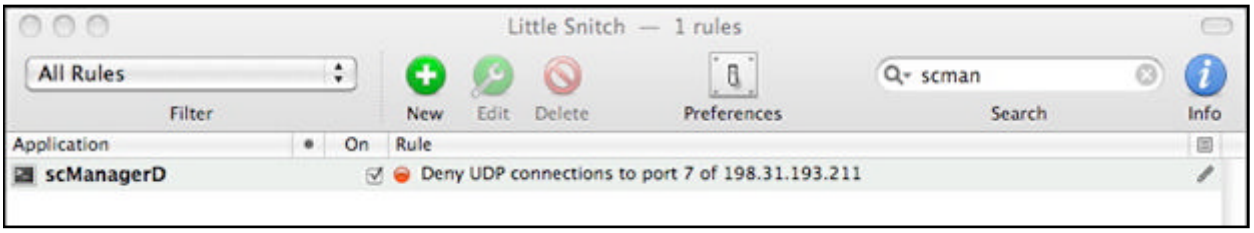
> ***Third-Party Sites***
>
> *Please note that other web sites that may be accessed when using our system may collect personally identifiable information about the end user. The information security practices of those third-party web sites accessed in conjunction with the Impulse Safe•Connect NAC System are not covered by this privacy statemen**t.***
>
> ***Cookies***
>
> *Impulse Point's NAC system or website do not use cookies. Accessing advertising or promotional web sites through the Impulse Point Portal may expose the end user to third-party cookies. If this is objectionable, the end user should set the permission levels at their browser accordingly. Impulse Point has no ability to monitor or control third-party cookie use.*

On first blush, these statements seem like generic disclaimers (and the second probably is just that). Yet, among other perplexing features (e.g., distinguishing between the operations of "other web sites" and "third-party cookies"), they offer loopholes big enough, as the saying goes, to drive a truck through. But this isn't hypothetical: ***I've seen the truck.*** And where it's headed is very interesting.

---

[34] Authored on Jul 17, 2007, 5:10pm by "dmuley", presumably Dennis A. Muley, Impulse Point's president.

After installing the Safe•Connect agent on my laptop, I observed on several seemingly random occasions that it (specifically, the executable file **scManagerD**, one of the two key executables embedded in the "Safe•Connect.app") tried to connect to a server at the IP address 198.31.193.211. Here is a screen capture of my interactive firewall's report of this:



These attempted connections were not limited to NSU's wireless network. They also took place on Columbia University's open wireless network and my own wireless network at home. This supports my earlier suggestion that Safe•Connect's activities extend beyond NSU's wireless networks.

That IP address translates into **host.onoc.net** under the domain **onoc.net**,[35] which is registered to DSM Technology Consultants, a "network of members firms of DSM Limited, each of which is a separate and independent legal entity"[36] — an unusually legalistic formulation for a website's footer. This would certainly appear to be a "third-party website" for the purposes of Impulse Point's privacy statement. However, Impulse Point LLC and DSM Technology Consultants share the same street address (6810 New Tampa Highway, Lakeland, Florida 33815) and up to six out of eight senior-most corporate officers with various titles (Principal, President, CEO, VP, COO, CSO), as well as one "executive assistant" (Impulse Point) cum "office manager" (DSM):[37]

---

[35] **host.onoc.net** is this IP address's canonical name ("CNAME"); it has at least one other alias (i.e., additional server name), **auth.impulse.com** — the server used for logging out for servers, as previously noted. The purpose of the domain-name system is to provide a "layer of abstraction" that allows network engineers to reorganize their networks without disrupting services. In normal practice, **scManagerD** would call a server by its hostname to give Impulse Point this flexibility. That it contacts an IP address at all, and one whose canonical name appears to be a third party, is reminiscent of Impulse Point's nondisclosure of its name in the preferences file that launches Safe•Connect.

[36] http://www.dsm.net/dsm/default.aspx . "ONOC" refers to "DSM['s] state-of-the-art Outsourced Network Operations Center (ONOC)."[29] [http://web.archive.org/web/20080705073300/http://www.dsm.net/Snapshot.pdf]

[37] Sources: *1.* Impulse Point LLC website, "About Us" [http://www.impulse.com/company.php]; *2.* Impulse Point LLC employees according to Educause [http://www.educause.edu/Community/MemDir/ImpulsePoint/35998]; *3.* DSM Ltd website "Leadership Team" [http://www.dsm.net/dsm/leadership.aspx]; *4.* e.g., DSM's website as archived on 2007-03-17 [http://web.archive.org/web/20070317140310/www.dsm.net/index.php?id=1_1]; *5.* e.g., DSM's website as archived on 2005-02-05 [http://web.archive.org/web/20050205195742/www.dsm.net/index.php?id=1_1]; *6.* Digital Systems Management's website as archived on 1997-04-09 [http://web.archive.org/web/19970409025528/www.dsm.net/pages/COINFO.HTML].

	IP [curr, *1*]	IP [n.d., *2*]	DSM [cur, *3*]	DSM [2007, *4*]	DSM [2005, *5*]	DSM [1997, *6*]
Alan Sebastian		Principal	VP, Consult Svcs	VP, Consult Svcs		
Dennis A. Muley	President	President			VP Sales & Mktg	
J. David Robinson	CEO		President			Pres, Client Svcs
Gene Thomason		VP				
Karl H. Muehlberger	COO		VP, Operations		Dir, Operations	
V. Maximillian Garcia	CSO					Designimation Sr D
Denis Edwards					CTO	
Brian Herzig	VP, Partner Dev					
Mike McMillan			Dir, Sys Integratn		Dir, Sys Integratr	Mgr, Tech Svcs
Anne Torgler		Mktg Mgr				
Jennifer Ireland		Bus Dev Mgr				
Genevieve Lapham		Regl Sales Mgr				
Peter Bonalos		Regl Sales Mgr				
Jack Trantham			Tech Consultant		Tech Consultant	Mgr AEC/ Designim
Kirk Anderson		Custr Service Spec				
Brett Hamill		Cust Service Rep				
Shelley Robinson		Mktg				
Barbara Stone		Exec Asst				Office Mgr

In short, the two companies seem to be distinguished in large part by the legal fictions of corporate entities. Moreover, two key people at the same address run yet another company that specializes in synthesizing data from numerous institutions, mining it, and visualizing the results.[38]

What I haven't attended to is the question, stated at the opening, of *what information this system discloses, to whom, and to what end.* I haven't yet been able to capture the data stream that the Safe•Connect agent tried to send to **host.onoc.net** (as noted, this behavior seems to be sporadic); and, in any case, I doubt that capturing it will be very useful, because it's probably encrypted.[39]

---

[38] Impulse Point and DSM Technology Consultants also share the same street address, at least two corporate officers (David Robinson and Karl Muehlberger [http://www.corporationwiki.com/Florida/Lakeland/intelimedix-llc-6379300.aspx]), and a phone number (863-802-8888) with another company, Intelimedix LLC. Intelimedix offers "data aggregation" and "advanced analytics [that] surfaces actionable intelligence" for the healthcare industry. [http://www.intelimedix.com/] They describe this as able "to overcome the challenges that arise when data formats differ and information must be exchanged with multiple organizations" [http://www.intelimedix.com/www/products.php], in ways that "identify status [...] with predictive modeling and statistical analyses [and] tailor messaging with analytics such as profiles." They add that "[h]osted analytics complement these solutions, while enterprise-wide analytic and reporting capabilities also are available." [http://www.intelimedix.com/www/products.php] In a 2008 USPTO trademark filing for the phrase "Drill Anywhere" (SN 77568650), Intelimedix stated that the phrase described "[c]omputer software that provides real-time, integrated business management intelligence by combining information from various databases and presenting it in an easy-to-understand user interface." While it's surely speculative to point this out, these services would be useful in synthesizing and analyzing other kinds data — for example, file-sharing data reported from numerous educational institutions — particularly if that data needed to be presented to a 'fourth-party' organization such as the RIAA.

[39] Disassembly reveals that **scManagerD** makes use of the "Blowfish" encryption algorithm, which is frequently used to secure communication channels.

Because the data stream is not available, I disassembled the **scManagerD** executable file that tried to send the data —a technical procedure involving extracting limited human-readable text from a compiled program.[40] Disassembled software is partial and can be cryptic, but in this case it is easy to identify contiguous code sequences that perform uncontroversial functions such as the ones NSU IT mentions (checking the IP address, DHCP gateway, and DNS server) as well as the computer's MAC address and hostname:

```
[line 14803] __ZN7NetInfo20GetSynthGatewayRouteER13NETINFO_ROUTE:
[line 14896] __ZN7NetInfo19SetDNSStringFromURLE7CStdStrIcE:
[line 14962] __ZN7NetInfo10GetIPTableERSt4listI7CStdStrIcESaIS2_EE:
[line 15009] __ZN7NetInfo13GetObservedIPEv:
[line 15029] __ZN7NetInfo13SetObservedIPE7CStdStrIcE:
[line 15044] __ZN7NetInfo10GetMacAddrER7CStdStrIcE:
[line 15063] __ZN7NetInfo10GetMacAddrEPhRm:
[line 15079] __ZN7NetInfo5GetIPER7CStdStrIcERhS3_S3_S3_:
[line 15115] __ZN7NetInfo5GetIPERm:
[line 15160] __ZN7NetInfo7GetDHCPERm:
[line 15397] __ZN7NetInfo13IsDHCPEnabledEv:
[line 15424] __ZN7NetInfo5GetIPER7CStdStrIcE:
[line 15442] __ZN7NetInfo10IsNetAliveEv:
[line 15458] __ZN7NetInfo7RefreshEv:
[line 15466] __ZN7NetInfo11GetHostNameER7CStdStrIcE:
[line 15506] __ZN7NetInfo10GetDNSListERSt6vectorI7CStdStrIcESaIS2_EE:
```

Similarly, it is easy to identify find code that could surveil *any and every* file on the computer by recording directory structure and files lists ("trees"), "fingerprint" them (with the MD5 cryptographic-hash function), and upload that data to a server:[41]

```
[line 11978] __ZN6Logger12GetTimeStampER7CStdStrIcE:
[line 12014] __ZN6Logger10WriteToLogEPKci:
[line 12080] __ZN6Logger8WriteLogEPKvPKci:
[line 12110] __ZN6Logger8WriteLogEPKvi:
[line 12125] __ZN6Logger8WriteLogEPKvR7CStdStrIcEi:
[line 12137] __ZN11MakeDirTree8MakeTreeE7CStdStrIcE:
[line 12292] __ZN11MakeDirTree12MakeFileTreeE7CStdStrIcE:
[line 12357a]__ZN9HashGroupD2Ev.eh,__ZZ11md5_processP11md5_state_sPKhE1w
[line 13263] __ZN11MD5Download23ConvertRawToHexChecksumER7CStdStrIcEPh:
[line 13305]  __ZN11MD5Download14GetHexChecksumE7CStdStrIcERS1_:
[line 13366] __ZN11MD5Download19DownloadAndValidateE7CStdStrIcES1_:
[line 13547] __ZN11MD5Download8DownloadE7CStdStrIcES1_S1_:
```

---

[40] Disassembling software has sometimes led to civil charges of infringement by copyright holders who argue that doing so is not covered by Section 117 of the Copyright Act, which provides limited exemptions for "owners" of the software in question. [http://www.chillingeffects.org/reverse/faq.cgi#QID191] However, because I did so in an academic context, and because my intent was to determine whether the executable contains malicious code, I believe that my inquiry is legitimate.

[41] Code running as root that can list running applications has access to *every* running application, and that code that can verify that particular files are present has access to *every* file.

Curiously, the logging, directory and file tree recording, and MD5 hashing take place *before* the network checks (lines 11978–13547 vs lines 14803–15506) that are widely claimed to be the Safe•Connect agent's primary service.[42] One consequence of this is that *data gathered through file-structure surveillance would probably be available for reporting as soon as the agent establishes that there is a network connection* ("IsNetAlive" in the previous block of code). In my observation (i.e., using forensic tools such as **lsof** ['list open files']), the Safe•Connect agent does not create any 'physical' files; thus, it's likely that any logs generated are stored in dynamic memory. This approach probably account for the unreasonable amount of dynamic memory that such an allegedly "lightweight" application consumes *at all times*.[43] (Such a design would also contribute to obscuring any undisclosed data-gathering by making it much more difficult to find the data.)

The preceding discussion does not address the second executable embedded in the "Safe•Connect.app," **scClient**. It too is launched when the computer boots, but unlike **scManagerD** it *can* be manually terminated and does not immediately relaunch itself. Its disassembled code suggests that it can perform 'interactive' functions such as displaying messages (presumably via a web browser, according to Impulse Point's literature). However, it too includes procedures for initiating communications with a "Server"; timestamping and logging; getting "Name", "DomainName", and "UserInfo"; forming XML on the basis of "TaggedItems"; and performing an "EraseEv[ent]." These procedures are too ambiguous to interpret.

Conclusion

In the course of my research, I've turned up more material than I've set forth in this document, which is already too long. In particular, it's been interesting to 'watch' — through archival and corporate research — DSM Technology Consultants engage in a series of exploratory business models over several years[44] as they established relationships with businesspeople and technicians working across a variety of fields. One notable aspect of this are the signs that their development essentially froze between around 2005. This is the period during which the corporate officers of DSM implemented Impulse Point LLC, despite

---

[42] If the Safe•Connect agent is indeed merely verifying the presence of antivirus software, there would be little or no advantage to translating a handful of directory and file names into MD5 hashes. An MD5 hash is a 32-character string, which might be only marginally shorter than directory and filenames themselves. If, on the other hand, **scManagerD** were scanning for hundreds or even thousands of large files (e.g., music files), such a procedure would be very advantageous in several ways. In particular, given that the most common P2P protocol, BitTorrent, requires synchronous uploading and downloading, this approach could work quite well. The protocol effectively requires that filenames remain unchanged while they're being shared, so the MD5 hashes of those names would remain unchanged as well — and therefore well suited to aggregation and analysis.

[43] As I write, the two component executables in the Safe•Connect agent, **scManagerD** and **scClient** are consuming 59MB of private address space — 150% of the memory consumed by the Mac OS's primary user-interface application, the Finder.app.

[44] These services were mainly centered on providing CAD services and running a data center focused on "businesses and governments in Central Florida." [http://www.dsm.net/dsm/about.aspx]

having little or no apparently relevant background for some of its key aspects, operations, and markets.[45] To this day, most of their promotional literature was created in 2006; and, indeed, their website (which was amateurish at the time and hasn't aged well) still states in its footer that it is "Copyright © 2006 Impulse Point All Rights Reserved."

A charitable interpretation of the evidence might run something like this: After exploring a variety of business models, the principals of DSM Technology Consultants hit on the idea of creating a wireless network access control system "designed for higher education's unique environment," and using it to distribute a software agent that can "scan [...] for music files as well as monitor all music files which are added to the computer [and] make any already downloaded illegal files unplayable." In conjunction with this, they received and/or compiled a "music library," a "block song list," a "fingerprint library," then developed "fulfillment links" and an "advertiser library" in order to promote the more widespread adoption of music obtained legally according to an industry trade lobby's demands. They incorporated Impulse Point LLC on April 5, 2004,[46] and for the first year promoted Safe•Connect system in these terms. However, when they found that the ability to "scan" others' computers and remotely make files "unplayable" was problematic, they substantially rewrote the software so that it could no longer destroy files, disposed of whatever aggregate data they had gathered, and repudiated any problematic exchanges of information with third parties such as the RIAA.

A cynical interpretation of the evidence is that when, in mid-2005, "Impulse Point" realized that some of the features they were promoting were problematic (and very probably illegal), they changed the wording of a few promotional PDFs but otherwise continued to look at higher-ed institutions as distribution points for spyware in the service of the RIAA and/or related interests. That the application is installed with root privileges at the system level; that it is always on; that is extremely difficult to uninstall; that it does not disclose its logging activities in the form of files written to disk; that it communicates directly with a "third-party" data center; and that it affects guests and unaffiliated parties — these are all *features not bugs*, as the saying goes.

As always, the truth probably lies somewhere in the middle. ***One possible step toward finding the truth would be to present Impulse Point with a series of reasonable questions:***

1. ***Does Impulse Point believe that FERPA restricts the Safe•Connect system's operations? If so, how? If not, why not?***
2. ***Are dsm.net, host.onoc.net, and any host under those domains "third-party" sites for the purposes of the Impulse Point Privacy Statement" and therefore "not covered by [that] privacy statement"?***

---

[45] The sole exception is Impulse Point COO and DSM VP Operations Karl Muehlberger, whose bio notes his involvement in "businesses [...] engaged in diverse fields from industrial manufacturing to music and entertainment to Internet companies." [http://www.dsm.net/dsm/leadership.aspx] [http://www.impulse.com/company.php]

[46] The Internet Archive copy of Impulse Point's www.impulse.com website as of September 13, 2003, redirects to DSM Technology Consultants' website www.dsm.net. [http://web.archive.org/web/*/http://www.impulse.com].

3. ***Does Impulse Point, DSM Technology Consultants, and/or any other commercial entity sharing corporate officers and the same street address provide any information gathered through Safe•Connect installations with any other party? If so, what information and with whom?***

4. ***Can Impulse Point provide a complete account of conditions under which the Safe•Connect agent communicates with servers other than the Safe•Connect Policy Enforcer resident at a host institution?***

Again, these questions are far from exhaustive.

I have made every effort to present this material and my analyses as factually and neutrally as possible. With the debatable exception of software disassembly, every fact reported here is based on publicly available information — most of it provided by the corporate officers of Impulse Point and DSM Technology Consultants. In particular, I have sought to frame this material and narrative in terms of questions that consistently emphasize NSU's history, mission, and best interests.

Moreover, I fully appreciate the fact that NSU is subject to a wide variety of laws, and that some of them require it to institute systems and procedures that may not be seen as conducive to abstract ideas about academic freedom. Specifically, the ''Higher Education Opportunity Act'' of 2008 (H.R. 4137[47]) requires "institution[s to certify] that [they] '(A) [have] developed plans to effectively combat the unauthorized distribution of copyrighted material, including through the use of a variety of technology-based deterrents; and '(B) will, to the extent practicable, offer alternatives to illegal downloading or peer-to-peer distribution of intellectual property, as determined by the institution in consultation with the chief technology officer or other designated officer of the institution.'" There is little doubt that the adoption of the Safe•Connect system is a good-faith effort to meet this legal obligation. ***However, it is reasonable to ask whether this system exceeds NSU's legal obligations — and, if so, what additional risks that may entail.***

A shared computing environment involves a delicate balance whose fulcrum is trust. IT staff must trust that the majority of its users are using shared resources legitimately; and users in turn must trust that IT staff maintain an environment in which neutrality and confidentiality are norms in deepest sense. As I noted at the outset, the Safe•Connect system dramatically shifts this balance. NSU IT explains the new policy in the following unfortunately careless terms when users first try to log in:[48]

> In order to ensure a safe computing environment for all users of the campus network, all computers are required to install and run various software to ensure a safe computing environment (anti-virus software, appropriate security patches, etc.). To ensure compliance, we require that all users install a software policy key. [...]
>
> If you click "I DO NOT ACCEPT" you will not have internet access.

---

[47] http://thomas.loc.gov/cgi-bin/bdquery/z?d110:h.r.04137:

[48] http://www.newschool.edu/at/network/wireless/SafeConnect_Install_Instructions.html

There are many things that could be said about this style of communicating with members of the NSU community, but the bottom line says it all.

Internet access has become a fundamental part of effective participation in the NSU for students, faculty, and staff alike. For now, the Safe•Connect system is required only for wireless internet access; but of course many of the stated justifications for Safe•Connect — concerns about viruses and spyware — apply equally to the 'wired' ethernet network as well. If NSU IT intends to require Safe•Connect only on for wireless access, then either the policy or its stated justification makes little sense. However, if NSU IT plans to require it for wired access as well later on, then users who do not accept it *will not have internet access.* ***Thus, it's reasonable to ask whether the implementation of Safe•Connect actively and equitably supports the NSU's primary mission as an educational institution.***

In closing, I believe that there are enough serious questions about Safe•Connect to justify suspending its implementation pending further review. I hope that the Provost's Office will work with NSU IT to address these questions, and do so in the most open and transparent manner. For example, if NSU chooses to present Impulse Point with specific questions, I hope that it will do so with the understanding that Impulse Point's answers will be made public. Safe•Connect affects hundreds of thousand of others at higher-ed institutions across the US, many of them public; as such, these are matters of *public interest*. If Impulse Point is able to provide clear, consistent, and convincing answers, that will benefit them; if they cannot, then other higher-ed institutions should have the opportunity to consider that in evaluating Impulse Point and the Safe•Connect system.

I thank your for your time and attention, and I look forward to your response.

Regards,
Ted Byfield