

MAGAZINE

# BSD

FOR NOVICE AND ADVANCED USERS

## Best of

# BSD ROB SOMERVILLE'S COLUMN COLLECTION

VOL.4 NO.02

1898-9144



855-GREP-4-IX  
[www.ixsystems.com](http://www.ixsystems.com)  
Enterprise Servers and Storage  
for Open Source



- ✓ Rock-Solid Performance
- ✓ Professional In-House Support

# FREENAS MINI STORAGE APPLIANCE

IT SAVES YOUR LIFE.



## HOW IMPORTANT IS YOUR DATA?

Years of family photos. Your entire music and movie collection. Office documents you've put hours of work into. Backups for every computer you own. We ask again, *how important is your data?*

## NOW IMAGINE LOSING IT ALL

Losing one bit - that's all it takes. One single bit, and your file is gone.

The worst part? **You won't know until you absolutely need that file again.**



*Example of one-bit corruption*

## THE SOLUTION

The FreeNAS Mini has emerged as the clear choice to save your digital life. **No other NAS in its class offers ECC (error correcting code) memory and ZFS bitrot protection to ensure data always reaches disk without corruption and never degrades over time.**

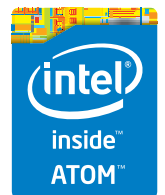
No other NAS combines the inherent data integrity and security of the ZFS filesystem with fast on-disk encryption. No other NAS provides comparable power and flexibility. The FreeNAS Mini is, hands-down, the best home and small office storage appliance you can buy on the market. **When it comes to saving your important data, there simply is no other solution.**

### The Mini boasts these state-of-the-art features:

- 8-core 2.4GHz Intel® Atom™ processor
- Up to 16TB of storage capacity
- 16GB of ECC memory (with the option to upgrade to 32GB)
- 2 x 1 Gigabit network controllers
- Remote management port (IPMI)
- Tool-less design; hot swappable drive trays
- FreeNAS installed and configured



<http://www.ixsystems.com/mini>



# FREENAS CERTIFIED STORAGE



With over six million downloads, FreeNAS is undisputedly *the* most popular storage operating system in the world.

Sure, you could build your own FreeNAS system: research every hardware option, order all the parts, wait for everything to ship and arrive, vent at customer service because it *hasn't*, and finally build it yourself while hoping everything fits - only to install the software and discover that the system you spent *days* agonizing over **isn't even compatible**. Or...

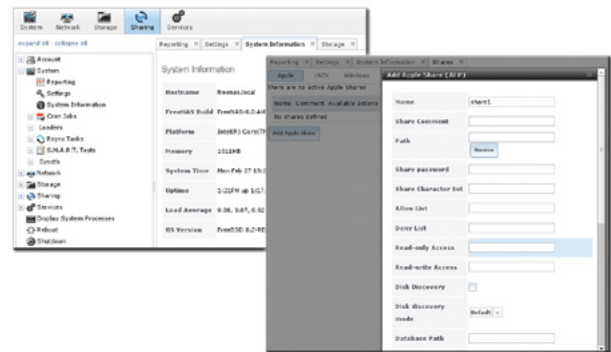
## MAKE IT EASY ON YOURSELF

As the sponsors and lead developers of the FreeNAS project, iXsystems has combined over 20 years of hardware experience with our FreeNAS expertise to bring you FreeNAS Certified Storage. **We make it easy to enjoy all the benefits of FreeNAS without the headache of building, setting up, configuring, and supporting it yourself.** As one of the leaders in the storage industry, you know that you're getting the best combination of hardware designed for optimal performance with FreeNAS.

## Every FreeNAS server we ship is...

- » Custom built and optimized for your use case
- » Installed, configured, tested, and guaranteed to work out of the box
- » Supported by the Silicon Valley team that designed and built it
- » Backed by a 3 years parts and labor limited warranty

As one of the leaders in the storage industry, you know that you're getting the best combination of hardware designed for optimal performance with FreeNAS. **Contact us today for a FREE Risk Elimination Consultation with one of our FreeNAS experts.** Remember, every purchase directly supports the FreeNAS project so we can continue adding features and improvements to the software for years to come. **And really - why would you buy a FreeNAS server from *anyone* else?**



### FreeNAS 1U

- Intel® Xeon® Processor E3-1200v2 Family
- Up to 16TB of storage capacity
- 16GB ECC memory (upgradable to 32GB)
- 2 x 10/100/1000 Gigabit Ethernet controllers
- Redundant power supply

### FreeNAS 2U

- 2x Intel® Xeon® Processors E5-2600v2 Family
- Up to 48TB of storage capacity
- 32GB ECC memory (upgradable to 128GB)
- 4 x 1GbE Network interface (Onboard) - (Upgradable to 2 x 10 Gigabit Interface)
- Redundant Power Supply



<http://www.iXsystems.com/storage/freenas-certified-storage/>

Dear Readers,

**W**e created one more issue for you that includes a collection of Rob's columns. I hope you will enjoy it and it will remind you of the best stories over the past few years.

*If you think that there is a topic worth publishing in a similar type of best of issue, please feel free to contact me.*

*Enjoy reading,  
Ewa & BSD team*

## Biography

*Rob Somerville has been passionate about technology since his early teens. A keen advocate of open systems since the mid-eighties, he has worked in many corporate sectors including finance, automotive, airlines, government and media in a variety of roles from technical support, system administrator, developer, systems integrator and IT manager. He has moved on from CP/M and nixie tubes but keeps a soldering iron handy just in case.*

*Enjoy reading,  
Ewa & the BSD team*

# MAGAZINE BSD

#### Editor in Chief:

Ewa Dudzic  
ewa.dudzic@software.com.pl

#### Contributing:

Michael Shirk, Andrey Vedikhin, Petr Topiarz,  
Charles Rapenne, Anton Borisov, Jeroen van Nieuwenhuizen,  
José B. Alós, Luke Marsden, Salih Khan,  
Arkadiusz Majewski, BEng, Toki Winter, Wesley Mouedine  
Assaby, Rob Somerville

#### Top Betatesters & Proofreaders:

Annie Zhang, Denise Ebery, Eric Geissinger, Luca  
Ferrari, Imad Soltani, Olaoluwa Omokanwaye, Radjis  
Mahangoe, Mani Kanth, Ben Milman, Mark VonFange

#### Special Thanks:

Annie Zhang  
Denise Ebery

#### Art Director:

Ireneusz Pogroszewski

#### DTP:

Ireneusz Pogroszewski  
ireneusz.pogroszewski@software.com.pl

#### Senior Consultant/Publisher:

Paweł Marciniak  
pawel@software.com.pl

#### CEO:

Ewa Dudzic  
ewa.dudzic@software.com.pl

#### Publisher:

Hakin9 Media SK  
02-676 Warsaw, Poland  
Postepu 17D  
Poland  
worldwide publishing  
editors@bsdmag.org  
www.bsdmag.org

Hakin9 Media SK is looking for partners from all over the world. If you are interested in cooperation with us, please contact us via e-mail: editors@bsdmag.org.

All trademarks presented in the magazine were used only for informative purposes. All rights to trademarks presented in the magazine are reserved by the companies which own them.

# FreeNAS

## in an Enterprise Environment

**NEW RELEASE**

By the time you're reading this, FreeNAS has been downloaded more than 5.5 million times. For home users, it's become an indispensable part of their daily lives, akin to the DVR. Meanwhile, all over the world, thousands of businesses, universities, and government departments use FreeNAS to build effective storage solutions in myriad applications.



### What you will learn...

- How TrueNAS builds off the strong points of the FreeBSD and FreeNAS operating systems
- How TrueNAS meets modern storage challenges for enterprise

**WE INTERRUPT THIS MAGAZINE TO BRING YOU THIS IMPORTANT ANNOUNCEMENT:**

THE PEOPLE WHO DEVELOP FREENAS, THE WORLD'S MOST POPULAR STORAGE OS, HAVE JUST REVAMPED TRUENAS.

The FreeNAS operating system is free, open source, and available to the public and offers thorough documentation, a large and active community, and a feature-rich storage environment. Based on FreeBSD, FreeNAS can share over a host of protocols (SMB, NFS, FTP, iSCSI, etc) and features an intuitive web interface, the ZFS file system, a plug-in system for backup, and much more.

Despite the massive popularity of FreeNAS, many aren't aware of its big brother, TrueNAS. TrueNAS is the data in some of the most demanding and complex enterprise environments: the proven, enterprise-grade, professionally-supported line of TrueNAS storage systems.

But what makes TrueNAS different from FreeNAS? Well, I'm glad you asked...



### Commercial Grade Support

When a mission critical storage system goes down, an organization's whole operation can come to a halt. Whole community-based support (like FreeNAS) is free, but it can't always get an answer quickly and running in a timely manner. TrueNAS offers a dedicated support team that can help you get up and running that safely.

Created by the same team that developed FreeNAS.

**POWER WITHOUT CONTROL MEANS NOTHING. TRUENAS STORAGE GIVES YOU BOTH.**

- |   |  |
|---|--|
| <input checked="" type="checkbox"/> Simple Management   | <input checked="" type="checkbox"/> Self-Healing Filesystem            |
| <input checked="" type="checkbox"/> Hybrid Flash Acceleration                                 | <input checked="" type="checkbox"/> High Availability                  |
| <input checked="" type="checkbox"/> Intelligent Compression                                   | <input checked="" type="checkbox"/> Qualified for VMware and HyperV    |
| <input checked="" type="checkbox"/> All Features Provided Up Front (no hidden licensing fees) | <input checked="" type="checkbox"/> Works Great With Citrix XenServer® |

To learn more, visit: [www.ixsystems.com/truenas](http://www.ixsystems.com/truenas)



### POWERED BY INTEL® XEON® PROCESSORS

Intel, the Intel logo, Intel Xeon and Intel Xeon Inside are trademarks of Intel Corporation in the U.S. and/or other countries. VMware and VMware Ready are registered trademarks or trademarks of VMware, Inc. in the United States and other jurisdictions.

Citrix makes and you receive no representations or warranties of any kind with respect to the third party products, its functionality, the test(s) or the results there from, whether expressed, implied, statutory or otherwise, including without limitation those of fitness for a particular purpose, merchantability, non-infringement or title. To the extent permitted by applicable law. In no event shall Citrix be liable for any damages of any kind whatsoever arising out of your use of the third party product, whether direct, indirect, special, consequential, incidental, multiple, punitive or other damages.

The Computer Says “No”	<b>8</b>
With the Recent Revelation That the United States Spied on Angela Merkel and the Subsequent Outrage From Politicians – is this a Case of the “Lady Doth Protest Too Much”?	<b>10</b>
OPINION: With the UK government in collusion with the major search engines to censor 100,000 search terms to prevent child abuse, is the UK joining the ranks of the technological fascists?	<b>12</b>
Technology makes a wonderful slave but a cruel master. Both Amazon and Tesco, major retailers in the UK and worldwide have been severely criticised in the media for the use of technology to control and monitor staff excessively. As IT professionals, where do we draw the ethical line in the sand?	<b>16</b>
With the Collapse of Red Flag Software (the World’s Second-largest Linux Distributor) is the Dream of Linux on the Desktop Even Further out of Reach?	<b>18</b>
With Every Business a Target for a Security Attack, are Organisations Finally Grasping the Security and Data Protection Nettle or is the Issue Still Being Kicked Into the Long Grass?	<b>20</b>
With the Recent Announcement of the Widespread Heartbleed SSL Vulnerability is it Time to Reconsider who the Troublemakers Really are?	<b>22</b>
In a Surprise Decision, Europe’s Top Court has Ruled That Google can be Forced to Erase Links to Content About Individuals. Is History Repeating Itself Once Again?	<b>24</b>
A recent poster on <a href="http://www.theregister.co.uk">http://www.theregister.co.uk</a> lamented that with all the recent security failures and the increase of patching, IT is not fun any more. Are we facing a new dark period in the technology sector?	<b>26</b>
While it cannot be disputed that the World Wide Web and the Internet has helped in speeding up the advancement of globalization in eroding national barriers – is there a down side to mass connectivity?	<b>28</b>
Over twenty years ago, Mitchell Kapor, the founder and former C.E.O. of Lotus Development Corporation stated, “The question of what to do about Microsoft is going to be a central public policy issue for the next 20 years. Policy makers don’t understand the real character of Microsoft yet”. Has government and industry smelled the coffee yet?	<b>30</b>
The UK government is planning to put trolls in jail for up to two years. Is this a sensible approach in containing the darker side of human nature?	<b>32</b>
Is There a Difference Between Geeks and Nerds?	<b>34</b>
“If you’re moving information into the cloud, it just seems to me that all kinds of nasty activity could go on in there. I would take a Missouri approach and say – prove it to me, show it to me – how it’s more secure”.	<b>36</b>



**NET OPEN SERVICES** IS AN APPLICATION HOSTING COMPANY FOCUSED ON OPEN SOURCE APPLICATIONS MANAGEMENT IN HIGH AVAILABILITY ENVIRONMENT.

NET OPEN SERVICES IS PROUD TO PROVIDE A HIGH QUALITY SERVICE TO OUR CUSTOMERS SINCE 10 YEARS.

OUR EXPERTISE INCLUDES:

- CLOUD COMPUTING, PUBLIC, PRIVATE AND HYBRID CLOUD MANAGEMENT (OPENSTACK, CLOUDSTACK, RED HAT ENTERPRISE VIRTUALIZATION)
- REMOTE MONITORING AND MANAGEMENT 24/7
- NETWORKING AND SECURITY (OPEN BSD, IP TABLE, CHECKPOINT, CISCO,...)
- OS AND APPLICATION MANAGEMENT (FREE BSD, OPEN BSD, SOLARIS, UNIX, LINUX, AIX, MS WINDOWS)
- DATABASE MANAGEMENT (ORACLE, MYSQL, CASSANDRA, NOSQL, MS SQL, SYBASE...)
- MANAGED HOSTING IN CARRIER CLASS DATA CENTERS
- DISASTER RECOVERY



WE PROVIDE SERVICES IN EVERY STEP OF THE PROJECT LIFE, DESIGN, DEPLOYMENT, MANAGEMENT AND EVOLUTIONS. **NETOPENSERVICES** TEAM INCLUDES EXPERIENCED LEADERS AND ENGINEERS IN THE INTERNET SERVER INDUSTRY.

OUR TEAM HAS 15 YEARS OF EXPERIENCE IN DEVELOPING INTERNET INFRASTRUCTURE-GRADE SOLUTIONS AND PROVISIONING INTERNET DATACENTERS AND GLOBAL SERVICE NETWORKS TOGETHER.

WE OFFER EXCEPTIONAL HARDWARE SUPPORT AS SOFTWARE SUPPORT ON UNIX/LINUX AND OPEN SOURCE APPLICATION. **NETOPENSERVICES** DELIVERS THESE CUSTOM-BUILT LINUX AND UNIX SERVERS, AS WELL AS PRECONFIGURED SERVERS AND SCALABLE STORAGE SOLUTIONS, TO OUR CUSTOMERS. WE ALSO OFFER CUSTOM DEVELOPMENT AND ADVANCED-LEVEL UNIX/LINUX CONSULTING SOLUTIONS.

# The Computer Says “No”

Stanislav Petrov, the officer in command of the Russian Oko monitoring station, prevented global nuclear holocaust by disregarding a false positive alarm and subsequently not reporting this to his superiors in a timely fashion and delaying a knee jerk response. How much reliance can we place on technology and what are the implications for a society where computers are increasingly given ethical responsibility by proxy?

The Turing test is the classic yardstick by which the fragile interface between humans, silicon and the universe is measured. The question “Can computers think?” still causes considerable debate, and while the Turing test is based on the emulation of human characteristics, recent advances in quantum physics- especially quantum entanglement – have demonstrated a more complex universe than we can imagine. According to Bell’s theorem, information in our universe travels instantaneously. To simplify, two particles separated by considerable distance will display the same quantum behaviour as if a message has passed instantly between them. This empirically reinforces the argument that a butterfly flapping its wings in one corner of the earth has an effect elsewhere.

That observation aside, I refuse to accept the hypothesis that computers can think on a simple premise – computers do not have a conscience. Without a doubt, computers can fake intelligence, and I would even go as far as to say the argument that computers demonstrate a minute level of consciousness holds some water, provided the definition of consciousness is broad enough (for example being aware of the environment). But again this argument is faux, an emulation and bordering on sophistry. What is deeply concerning though, is the increasing mindless delegation of ethics, morality, decision making and authority to a piece of hot silicon in a data-centre somewhere. If Stanislav Petrov had not had the common sense to compare the false alarm against other criteria, we may not have been around today to have this discussion.

Unfortunately, since this information was released in 1974, as a civilization we have become considerably less aware of the dangers and much more dependent upon technology than ever before. The twin curse of commercial efficiency and profit-making have pushed us over the peak of the bell curve, and there is now no slack in the system for error. Just In Time production is a case in point. While in deeper reaches of the Internet those that defend preparedness are considered “Tin foil hatters”, the reality remains that in a modern Western society, we only have 24 hours food in the shops. Where I live in Great Britain, the situation is even worse as a substantial percentage of our food is imported from abroad, including Vietnam and Thailand.

Technology makes a great slave but a terrible master. The past 20 years bears witness to this – with the big bang in the financial sector, the decision making process in the marketplace was





increasingly delegated to technology, yet many times the plug has been pulled due to the system developing a form of hysteresis in that they were attempting to interpret new scenarios using inaccurate data and consequently failing miserably. While the recent financial crash cannot be laid squarely at the foot of technology, it is not a risk free strategy attempting to out-gun your competitors by means of brute speed alone. The recent demand in the financial sector for using higher speed backbones for communications purely on the basis that shaving a few milliseconds per transaction being the difference between a substantial profit or a spectacular loss, should raise alarm bells if that is the best strategy of your business sector.

I am stubborn in my belief that technology has immense benefits to offer mankind, but the more powerful the tool, the greater care one must take in its implementation and use. As a child, my father gave me a plastic tool-kit with plastic spanners, screwdrivers, etc. The havoc reigned with their real life counterparts in the hands of a 5 year old doesn't bear thinking about as the following tale will illustrate. As a young lad I owned a 12 volt Airfix power supply, and gaining access to my father's large metal screwdriver, I discovered that a substantial spark could be generated by shorting out the terminals. With uncontrolled ego and lust for excitement, I decided that the 240v AC emanating from the wall socket would make an interesting test case, and after procuring two 6 inch nails I managed to successfully circumnavigate the safety shutter and insert the aforementioned metallic items into the socket and

short them out. The resulting explosion and flash was indeed spectacular, and while both child and screwdriver survived, the nails and the considerably large fuse at the local substation (Rated somewhere between 100 and 600 Amps) did not.

While I am not implying that those who make the decision to wholly migrate from manual systems have the mentality of children, there is a widespread fallacy in management circles that technology alone can solve all the problems. Yes it can help, but with one im-

portant proviso – that human beings are able to interpret the results and override the system as necessary. Ideally, technology should be democratic rather than fascist, an educated voice rather than capturing the entire decision making process and expediting the result via a closed interface that cannot be overridden. Thankfully some industries understand this well, most modern trains and passenger aircraft are fly by wire and very safe. However, there are always trained pilots or drivers on hand to take control if the unexpected does happen, and it is a statistical guarantee that it will.

Where the problem arises is when management, the shareholders or whoever decide that “the automated system” will become the de-facto ethical and moral standard – removing the human element and as a consequence any common sense. You can code all the algorithms you like, but you cannot replace the breadth of human experience, understanding and wisdom. Again, the Internet proves this, we have unparalleled access to data but extrapolating the kernel of truth from the propaganda, opinion and noise makes quality information gathering difficult.

The badly designed script driven call centre is probably the best analogy to describe this scenario. Using a set of computer based rules, the operator is constrained by company policy and lack of autonomy – if the computer says “No” there is no chance of appeal, unless of course you manage to capture the ear of a sympathetic manager. Senior management are unaware of the level of gross customer dissatisfaction, as the metrics cannot reflect the moral offence of a human relaying a decision made by a lump of metal, effectively de-humanising the interaction. Rather than improving customer service and efficiency, the opposite occurs shortly followed by a battalion of fire-fighting reputation managers and PR gurus when the wheels fall off.

I propose we name this stupidity in honour of the man who saved countless millions of lives “The anti-Petrov effect”.

---

## ROB SOMERVILLE

*Rob Somerville has been passionate about technology since his early teens. A keen advocate of open systems since the mid eighties, he has worked in many corporate sectors including finance, automotive, airlines, government and media in a variety of roles from technical support, system administrator, developer, systems integrator and IT manager. He has moved on from CP/M and nixie tubes but keeps a soldering iron handy just in case.*

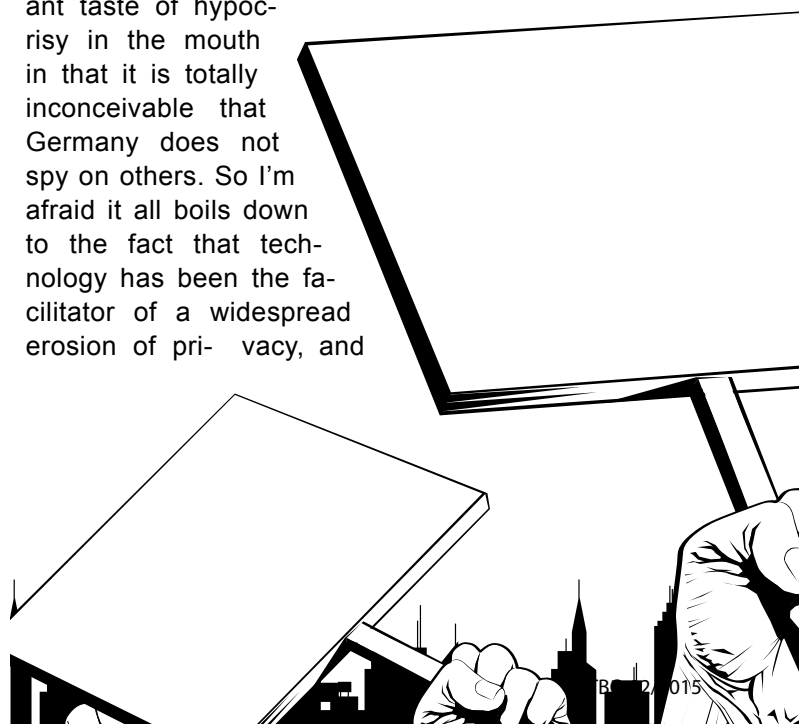


## With the Recent Revelation That the United States Spied on Angela Merkel and the Subsequent Outrage From Politicians – is this a Case of the “Lady Doth Protest Too Much”?

Here in the United Kingdom, we are well ahead of the game that the USA, the German leader, Angela Merkel, and the media is currently playing the game of faux outrage and hurt feelings over the surveillance of telephone conversations by the USA of 33 world leaders. After all, the scandal which has been simmering away for the past few years concerning the hacking of phone messages by News International culminating with the Leveson enquiry (and the subsequent recommendations that press freedom be legally curtailed) is not latest news. While quite rightly there was outrage that the media used such underhand tactics against the general public, politicians, celebrities and even the Royal Family, the other side of the argument has had scant coverage – that we live in a very different society from Victorian times.

**Y**ou might be shocked at my blatant anchoring of loss of privacy values prior to the publication of George Orwell’s masterpiece 1984 in the post war years, but please bear with me. Casting aside the fact that Government, Kings and the Church have used spies throughout history, the Victorian age was the last epoch where the average man, woman or child could be guaranteed a relatively strong sense of privacy. That is why I must take Angela Merkel’s “outrage” with a pinch of salt the size of a Siberian salt mine. Any politician who is unaware of the historical precedent of dirty dealings between warring states (or indeed allies) is either naive, uneducated or deceived, and even more so in the case of Angela Merkel who must be aware of the worst abuses of government power that took place over the border in East Germany by the Stasi during the Cold War. If I was to be generous, I’d say the outrage is driven by that historical fact but that leaves the unpleas-

ant taste of hypocrisy in the mouth in that it is totally inconceivable that Germany does not spy on others. So I’m afraid it all boils down to the fact that technology has been the facilitator of a widespread erosion of privacy, and



irrespective of political hue or ideal, any power will use that lever to their advantage where at all possible.

Let's get back to the Victorians. To send a letter (or to communicate) the letter was sealed, delivered and the recipient would break the seal and read the communication. Like the well proven process used by the Roman General, the unbroken seal on the scroll was the guarantee of authenticity, unless of course the senders credentials had been compromised. Forgery will always be the weak link in the chain, proving the identity of an individual with 100% accuracy always elusive, as the immoral can always get round this provided they have enough resource. The question "Who am I" extends past philosophical debate into real life wherever the identity of a person requires confirmation. So we can assume that privacy was reasonably well guaranteed unless there was sufficient reason to commit the offence of intercepting the Queens Mail, an offence that carried the death penalty.

From the 1900's up until the Second World War, the widespread adoption of the telegraph, telephone and radio communications muddled the field and this is where the root of the issue lies. The more people that are involved with the transmission of your message, the more open the transport medium used, the greater the coverage and penetration, the greater the chance your message is no longer private. Then came the Second World War. The necessity for documenting citizens became paramount in the interests of national security, and in the UK the adoption of the National Health Service and welfare state allowed a huge paper bank to develop of the characteristics of the general population. While crude, this database is the basis of the current conundrum – who can we trust to be the guardians of confidential data? Much has been made about NSA intercepts in that they are only interested in the meta-data – who is communicating with whom – rather than the message itself. On the face of it, that is a powerful rebuttal, but let's not forget in the age of the Strowger switch (used in telephone exchanges) it relatively easy to calculate who is connected to who.

While invented in the late 1800's, the first trial was not carried out in the UK until 1914. So the potential for capturing meta-data has been around at least since the early 1900's. What is revealing though is the notion of using the meta-data argument to support Internet snooping as it is historically part of both the spy's and detective's trade-craft. In reality, the concept of privacy died along with horse

and cart. Whether it be multi-nationals gathering marketing information, software manufacturers knowing your physical location or government reading your email, there are too many areas to cover. Sadly, by the time Orwell's book was published, the cracks had already started in the edifice of personal privacy, and while the Zeitgeist has been looking at the physical manifestations society wide, those that have the means, ability and reason to monitor have been increasing their power base under the radar (and I am being generous here) since the Second World War. What is truly telling though is the penalty for intercepting communications. In the Victorian age, the penalty was death. Today, a hefty fine and maybe a prison sentence will be your fate, despite the much greater opportunity for abuse. So I totally agree with the editor of the British satirical magazine Private Eye, Ian Hislop, that we have enough legislation as it is to combat any excesses of power, but the fact remains that there is one law for "them" and one law for "us". Angela Merkel has managed to capture the ear of the US President, and I suspect while an apology will be made and steps taken by the German government to improve domestic security, this is no comfort for the man in the street. The only comfort I can see is that while the USA has probably the most advanced spying infrastructure in the world today, at least this is offset to a small degree by a Freedom of Information culture that has teeth, and a legal system that is not afraid to sue even government. Other countries are not so fortunate. Angela Merkel as a world leader has an intelligence service and a legislature at her beck and call. No doubt there will be some major changes to European legislation on the back of this revelation. But this is all smoke and mirrors. Unless people truly appreciate we no longer live in the age of privacy, and the full weight of the law executed without bias to protect individuals, corporates and governments from abusive governments, corporates and individuals, we are all going to remain vulnerable, paranoid and an easy target. The concept of "who watches the watchers" has never been more apt.

## ROB SOMERVILLE

*Rob Somerville has been passionate about technology since his early teens. A keen advocate of open systems since the mid-eighties, he has worked in many corporate sectors including finance, automotive, airlines, government and media in a variety of roles from technical support, system administrator, developer, systems integrator and IT manager. He has moved on from CP/M and nixie tubes but keeps a soldering iron handy just in case.*

## OPINION: With the UK government in collusion with the major search engines to censor 100,000 search terms to prevent child abuse, is the UK joining the ranks of the technological fascists?

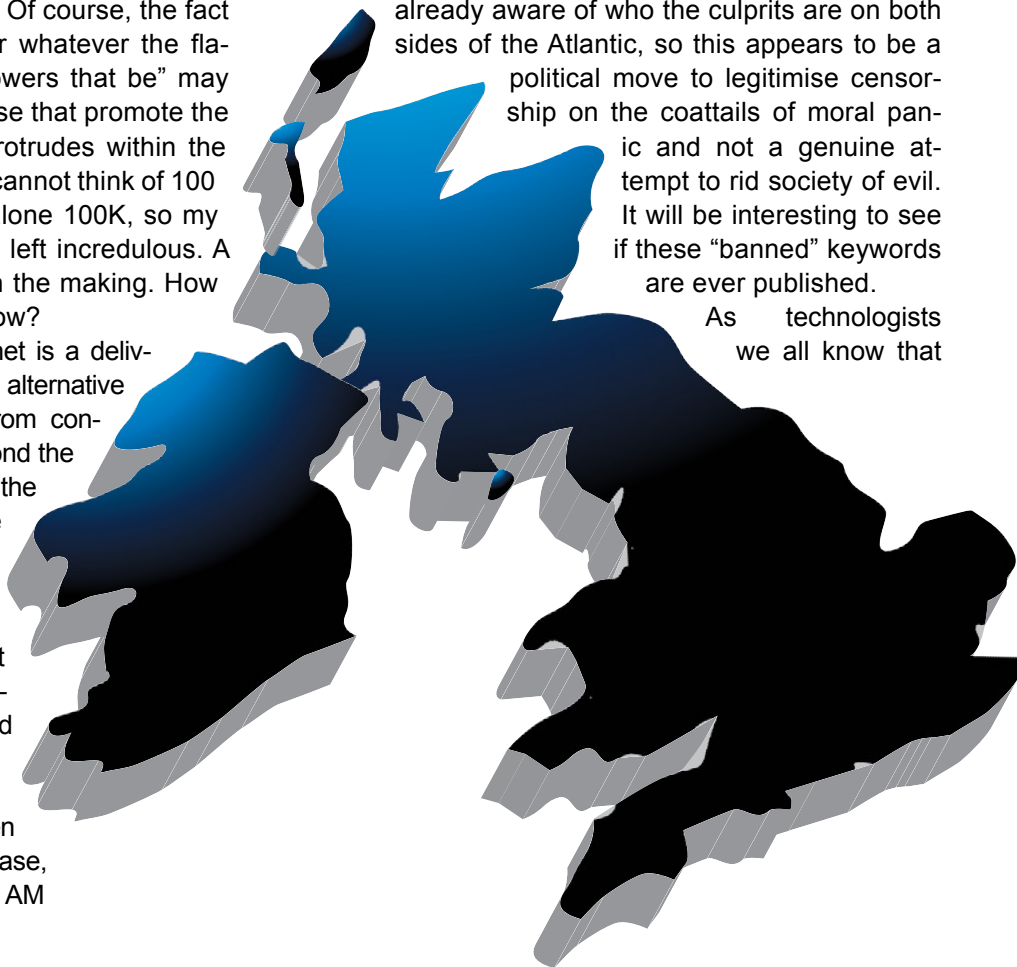
**D**avid Cameron, while no fool, by his authority as Prime Minister of the United Kingdom, has backed the censorship of 100K search terms alluding to child abuse in collusion with Google, Bing, and no doubt other search providers accessible in the UK. The exact extent of the legal framework is yet to be formalised, but it is clear that the UK government is moving towards a more proactive stance of censorship in a populist move to assuage the “something must be done to protect us from the Internet” lobby. Of course, the fact that political affiliations, terrorism, or whatever the flavour of the day that offends “the powers that be” may be added to this list has escaped those that promote the nose of this particular camel that protrudes within the tent of content delivery. Personally, I cannot think of 100 terms that relate to child abuse let alone 100K, so my inner skeptic, not unexpectedly, was left incredulous. A classic case of political disconnect in the making. How many words do Eskimos have for snow?

Contrary to popular belief, the Internet is a delivery system, not some monster with an alternative agenda to deprave and corrupt all from conceived embryos to the elderly and beyond the grave. It is a reflection of society. On the surface, triggering an alert if someone was to type “kiddie porn” into Google, seems a good way to deal with the totally abhorrent desire of an individual to have sexual relations with prepubescent children. What happens if you are a genuine journalist, researcher, concerned parent or a medical professional? Your browser gets an alert and your IP address is committed to a database. Then what? Questions are asked, or worse case, a visit by your local police force at 5:00 AM

to seize all Internet enabled devices, recordable media and a forensic investigation of every detail of your life and moral censure? The Internet is transient – a page can appear and disappear within minutes, or in the case of the current Conservative governments’ previous election promises – a few years. Thanks for nothing, Google. What is still unclear is how much of this data will be passed to other intelligence services or bodies via the NSA and GCHQ.

Let’s not be under any illusion here, the watchers are already aware of who the culprits are on both sides of the Atlantic, so this appears to be a political move to legitimise censorship on the coattails of moral panic and not a genuine attempt to rid society of evil. It will be interesting to see if these “banned” keywords are ever published.

As technologists we all know that



filtering search terms and attempting to categorise them intelligently is a pretty pointless exercise unless you throw massive human resources at it. During the miners' strike in the UK during the 80s, the eavesdropping system monitoring UK telephone conversations was overloaded due to the sheer weight of relevant data. I recently installed a corporate wide messaging system on our Intranet, and as a precaution to assuage the naysayers, added a swear filter knowing full well that it was a token gesture. If people want to do bad things, they will find a way to do them. This is IT help-desk 101. The fallacy that technology can be a moral guardian is rife with miscarriages of justice. Just ask any motorist who has been captured speeding by a badly aimed or calibrated speed gun or, indeed, a customer on the wrong end of a customer services "script". Technology is digital, black and white, whereas real life is analogue, a spectrum of colour. Here lies the perpetual paradox and argument between the spirit and the letter of the law. Unfortunately, history has proven that venal individuals can capitalise on this argument, be they defendants, prosecutors or, notably, governments.

So let's cut to the chase. Child pornography is evil. Anyone of sound mind caught manufacturing, distributing or consenting to such deeds should be quite rightly and with full weight, condemned not only in a court of law, but also in society. The basis of civilisation is innocence, innocent until proven guilty and the right to have a childhood of innocence. Anything else is a travesty.

Unfortunately, the law once again blindly overreaches in this regard, as possession in the UK of the worst type of pornography is a strict liability offence (i.e. you got it, you are guilty). While no cases to my knowledge have reached the courts here in the UK, the law is cut and dried – if you have "bad content" on your servers, you are liable. End of story. No *mens rea* (state of mind) appeal is allowed under strict liability cases. So as a system administrator in the UK, if I find objectionable 3<sup>rd</sup> party material on my server I run the risk of prosecution if I attempt to hand this material over to the authorities. So what should I do? Delete it and say nothing? In theory, no prosecuting authority would be so aggressive as to pursue such a case with a co-operating individual but in this age of febrile condemnation of the mass media and legalism, who knows? If somebody wanted to prove a point, all they need do is dump some images on a competitor's or political opponent's hard disk and make a few phone calls. The rules and ethics that work in the real physical world (e.g. possession of drugs) does not work with electronic data.

In reality, the neighbourhood paedophile is protected. They are either using strong encryption or are part of a network that is peer to peer, either electronically or socially. The level of social disgust that is associated with this issue means that it is now the holy grail of the blackmailer or the foreign government as sexual preferences, political alliance and financial corruption are now regarded as issues that are of little social consequence – unlike during the days of the Cold War. To any rational mind, a government or their intelligence services wanting to widely discredit an individual will aim for smearing with this particular human frailty. This adds an interesting dimension to the English phrase "Conspiracy or cock-up". Blackmail or media slaughter anyone? So, to truly defeat this evil in our society, we need a decent whistle-blowing strategy, and properly resourced root and branch investigations, not the crude hammer of the law that condemns due to content possession irrespective of motive.

The recent Jimmy Savile scandal proves this, in that victims were scared of coming forward and when they did, they were discredited or ignored often because of the position of privilege held by their abusers. Pauper or king, for justice to prevail, all need to be treated equally

under the law. Sadly, this is not the case. God help an innocent ISP or a victim under the current legislation.

David Cameron's febrile attempt at cleaning up the Internet proves beyond all doubt that he doesn't understand the issues. Over 90% of child abuse victims know their abuser socially. Granted, the Internet is a medium that allows people to build relationships, but to categorise an individual as deviant by what request they submit to a search engine is not only an abuse of process, but an abuse of power. And that doesn't take into account the malware a reasonably skilled IT engineer could build to generate a spoof of an individual's request. This move plays right into the hands of the spammers and the criminal underworld, allowing them to blackmail ordinary citizens with false accusations. "You have been looking at illegal content. Send us your credit card details and £250 or we contact the authorities". No paedophile is going to be searching for the type of content they desire using a search engine – it is more likely to be distributed via peer-to-peer or stored on a server within the Tor network. The truly paranoid would send it via snail mail on an encrypted USB stick or CDROM. So this cure will create more problems than it solves.

So what can we do about this evil as a community? First of all, we all need to be aware of and identify all the different types of low-life that are out there – fraudsters, sock-puppets, trolls, spammers, bandwidth abusers and copyright infringers, *et al* irrespective of whether we are IT professionals or end users. Birds of a feather flock together. I am not generally talking about individuals here, as we are probably all guilty at some point of committing some of these actions to a lesser degree. Who hasn't filled in a web-form with false details or used the corporate network to download an MP3 or two? I am talking about the communities that make a lifestyle, political or commercial choice to do such things en-mass on a regular basis causing disruption and distress to all.

We need a mechanism to quickly electronically disable and deal with these communities in law. If you get 500 phishing emails a day, that is 500 counts of attempted fraud, but will law enforcement take it seriously? Due to the distributed nature of networks, while the malware causing the problem may be on 500 individuals' PC's, it is not necessarily true that they are guilty of anything other than bad security hygiene. It is the authors and bot-masters who are guilty. We need a segregation of legal adult content into a XXX domain that is easily blocked by parental controls, backed by legislation that pursues the owner of the domain (e.g. the content owner) for breach. The province of the purchaser can then easily be proved in a court of law, absolving the ISP of responsibility. After all, like an

estate agent or realtor they are only selling space, they are not responsible for the acts that take place inside the property. Of course, if the ISP does discover illegal activity, they have a duty to report it. Still, as mentioned earlier, in the UK at least it is not that easy. The same idea could apply for global financial transactions etc., but of course certain vested interests want to have their cake and eat it, in that they want global freedom without necessarily any accountability or responsibility.

So a global Internet wide agreement is probably never going to happen.

Another approach is on a country by country basis. Once again, this has its dangers. I don't want some policy maker deciding if I can visit [www.ihatemygovernment.org](http://www.ihatemygovernment.org) (Yes. It exists). China and Google firewalls anyone? Anyway, any experienced IT user can proxy or tunnel their way around it.

No, the Internet, like rain, sunshine and death is available to everyone, including paedophiles. The maxim "I disapprove of what you say, but I will defend to the death your right to say it" needs to be revisited and reconsidered as in 2013 we don't just have words but images and video available to all as well. While freedom of expression is vitally important we equally need social, moral and legal responsibility, from the tramp to the millionaire. We live in a wonderful age, where barriers are collapsing and we can connect and understand more than the shallow political rhetoric that has dominated the last 2000+ years. What matters most is what people and society values – in real life and online. Until we get some cohesive action and the issue of Internet crime is taken seriously just as it would be on the street, WWW will continue to stand for Wild Wild West.

---

## ROB SOMERVILLE

*Rob Somerville has been passionate about technology since his early teens. A keen advocate of open systems since the mid-eighties, he has worked in many corporate sectors including finance, automotive, airlines, government and media in a variety of roles from technical support, system administrator, developer, systems integrator and IT manager. He has moved on from CP/M and nixie tubes but keeps a soldering iron handy just in case.*

“IN SOME CASES  
**nipper studio**  
HAS VIRTUALLY  
**REMOVED**  
the **NEED FOR** a  
**MANUAL AUDIT**”  
CISCO SYSTEMS INC.

Titania's award winning Nipper Studio configuration auditing tool is helping security consultants and end-user organisations worldwide improve their network security. Its reports are more detailed than those typically produced by scanners, enabling you to maintain a higher level of vulnerability analysis in the intervals between penetration tests.

Now used in over 65 countries, Nipper Studio provides a thorough, fast & cost effective way to securely audit over 100 different types of network device. The NSA, FBI, DoD & U.S. Treasury already use it, so why not try it for free at [www.titania.com](http://www.titania.com)



## Technology makes a wonderful slave but a cruel master. Both Amazon and Tesco, major retailers in the UK and worldwide have been severely criticised in the media for the use of technology to control and monitor staff excessively. As IT professionals, where do we draw the ethical line in the sand?

**T**o quote Albert Einstein, “Technological progress is like an axe in the hands of a pathological criminal.” Time and again throughout history, as a society we have seen the positive contributions made by innovators, creatives, engineers, architects and humanitarians perverted and used for immoral if not evil ends. Tempting though it would be to take Einstein’s quote and neatly assign to the technologists the role of the angels and to the politicians, bankers, society or whoever else the role of the pathological criminal, this would be far too simplistic. As far as I am concerned, the actions of black-hat hackers, spammers and the various other forms of Internet low-life are definitely criminal if not pathological. Of course, we must make allowances for the uneducated and the unaware, and I do not include here the average end user who has a compromised PC due to poor web hygiene. No, we are talking about those whose hearts are dark and who choose to use technology for their own agenda, rather than for the benefit of all.

Traditionally, the guru was party to esoteric knowledge shared with others either for financial, spiritual or social status. The first rule for the guru was the protection of knowledge and wisdom, as it was widely understood that the value of the guru would be inversely proportional to the number of people who were cognisant to the “magic”. Essentially, the same morality exists today in the form of the established professions – Doctors, Lawyers, Architects etc. – the amount of studying, self-sacrifice and knowledge that is required to achieve qualifica-

tion and recognition is great, so the profession then erects barriers to those that are not initiated. This in turn leads to separation within society, between those with the knowledge and as a consequence – power – and those that do not. This has led to cries from the “have nots” of injustice, and so the political ideologies of Marxism, Communism, Maoism, Stalinism, Socialism etc. gained traction and political credence in the 20th century. Irrespective of the basis of these riches, whether they be intellectual, financial, or physical, there were secrets to keep, professional relationships to be nurtured and at all costs the status quo to be maintained.

Aside from political argument as to whether or not Capitalism or any other doctrine is superior, the second rule for the guru is do not whistle-blow. Ever. The consequences of being an initiate and sharing “dirty washing in public” range from censure, character assassination to potentially death depending on the quality, importance and potential embarrassment caused by the information being shared. Just ask Frank Serpico. Unfortunately we cannot ask Karen Silkwood. Of course, if “leaking” information is useful to discrediting another guru, often this will be encouraged.

So I have no problem at all of awarding Edward Snowden the author’s “IT Man of the year” award for courage, honesty and integrity but qualified with a very small pinch of salt. While it is difficult to get to the bottom of any spook-based operation, especially taking into account the incestuous relationship the media (including the alternative media) have with the security services, it is hard to



reconcile on a pragmatic basis why ES chose to seek asylum in Russia. Maybe it was the harsh hand of fate, the bitter cup of circumstance that placed him in these circumstances. Unless this becomes public knowledge, or we manage to share a cup or two of coffee I doubt I will ever know. But if I was in his shoes, I would have chosen a host that couldn't potentially change his role from truth-teller to political pawn a la the exchanges that happened on the borders of East and West Germany during the cold war. We mustn't judge though – as far as I am concerned

to discuss, please feel free to email me at [me@merville.co.uk](mailto:me@merville.co.uk)). Others are more comfortable bearing their heart in short bursts. I aim for 1000 words. Maybe, I am a dinosaur, but as I mentioned earlier context is everything, and that is why every guru has to take his personal path to enlightenment. Only you know from your personal value system if the project you are working on is a threat. Does it pass the smell factor? How uneasy do you feel? Could you justify it in front of your manager? The CEO? The shareholders? Society? The universe? God?



ES has made a tremendous sacrifice and we must honour that irrespective of the geopolitical rhetoric. In my book, truth-teller, whether communist, fascist or capitalist must be applauded wholeheartedly.

But lets get back to reality, rather than a media frenzy of accusation and counter accusation. The problem with committed IT professionals (and I use the word committed here in the sense that we are passionate rather than candidates for the lunatic asylum) is that what we are involved with is often in the scale of rocket science, nuclear physics or whatever. A few thousand lines of code can change lives. Our product can be the stiletto that is used to shave 20% off the staffing levels of an organisation, or maybe as system administrators we can be asked to forget major “ethical hiccups”. And some of us write code for nuclear weapons guidance systems. When you are submerged in lines of code, caught in the political management cross-fire with a serious deadline due, or just burnt out with the whole shebang, it is important to remember the context, despite how difficult that is to do.

Like all of society, IT has its mix of extroverts and introverts. Personally, I prefer quality over quantity, so I spend my time writing long leader columns that will hopefully entertain and communicate rather than lots of spurious noise on Facebook and Twitter. Sheesh, I don't even have a blog. So in Internet terms, I am probably a confirmed introvert (I do occasionally reply to emails. If you have any constructive comments on these columns, or would like

To be honest, I feel sorry for the coders and techs involved in the Amazon and Tesco projects. Payback in the form of negative media exposure, no matter how distanced you are from the source or target is never pleasant. At the time, everything was probably justified from a management and project perspective, but naturally hindsight has 20-20 vision. In all my years as a tech, apart from those leaning towards or in management, I have never met an IT specialist who wanted to see jobs lost or benefits reduced by the application of technology. Maybe I have worked with too many idealists, but we all wanted to make things better. Safer. More productive. Less stressful. More fun. And at the same time make an honest buck. So let's raise our glasses in New Year 2014 to the Snowdens, Assanges, Tesco and Amazon employees who have had the courage to blow the whistle. And may they be our encouragement to do likewise as we enter deeper into the age of the pathological criminal.

---

## ROB SOMERVILLE

*Rob Somerville has been passionate about technology since his early teens. A keen advocate of open systems since the mid-eighties, he has worked in many corporate sectors including finance, automotive, airlines, government and media in a variety of roles from technical support, system administrator, developer, systems integrator and IT manager. He has moved on from CP/M and nixie tubes but keeps a soldering iron handy just in case.*

# With the Collapse of Red Flag Software (the World's Second-largest Linux Distributor) is the Dream of Linux on the Desktop Even Further out of Reach?

**W**hen Red Flag Linux was launched in 2007, there was much fanfare in the Open Source community. The most populated country in the world had embraced the vision, backed by government, and even a grudging olive branch had been thrown towards Microsoft in developing a Windows XP like interface. What could possibly go wrong? At time of writing it is unclear exactly why the project collapsed so spectacularly; some cite the Chinese Academy of Sciences' removal of funding due to the competition from Red Hat and SUSE Linux. What is clear however, is that another large government backed computer project has fallen by the wayside.

This is a sad day for the Open Source movement. While the cynical amongst us may suspect back doors and all sorts of underhanded compromises that go hand in hand with government surveillance and not shed a tear over the demise of Red Flag from an ethical perspective, the fact remains that domination of the world's largest marketplace is back in the hands of commercial interests, other than the enlightened few stalwarts that decide to download their own software – that is, of course, if it is available via government controlled firewalls or via a DVD from a friend. Under the circumstances it would be hard to accept a score other than Communism 0 – Capitalism 1.

Anyone with a scintilla of commercial reality understands that the desktop is dominated by Microsoft, as the majority of corporations have adopted MSC solutions. This popularity has spread across to the consumer marketplace but with one exception – mobile and tablet devices. In the early age of the motor car, the market was dominated by Ford with their innovative vision of mass production. Everyone else then followed suit and, to this day, very few independent motor manufacturers remain. But where does Ford rank today? Well behind General Motors, Volkswagen and Toyota in terms of production.

So the cyclical curse of the capitalist marketplace once again claims another scalp – the innovator, the creative – once on top doesn't always finish first. So maybe MSC isn't in such a strong position after all.

MSC is at a critical juncture in its history. There is a serious move away from the classic in-house desktop / server relationship with the success of tablets and mobile phones. Organisations are thinking more and more along the lines of remote desktops, virtualisation and bring your own device. Maybe the question isn't what Operating System will dominate the desktop, but what method will be used to deliver applications? If the move towards thin-client takes off, MSC will need to morph away from its traditional model for the corporates – Servers, Desktops, Applications, and Developer tools.

There is another issue at stake here, apart from the ethical issues of moving applications and data off to some server farm somewhere. Windows 8, like Ubuntu Unity, has caused consternation amongst the old school by radically re-designing the user interface in an attempt to bring cohesion across devices. It has been a Marmite moment – you either love it or hate it. At the moment, the corporates hate it, and those who are not committed to the change from a Start button or classic menu anchored to the top or bottom of the screen struggle. I recently had to explain to a friend, who had purchased a new consumer-grade laptop with Windows 8 installed, that he was basically stuck with it unless he forked out for a Windows 7 licence – a discussion that involved much swearing and slapping of the forehead. Friends come and go, but enemies accumulate and MSC is building a dedicated following of the latter with its short-sighted "Our way or the highway" mentality.

Microsoft's nemesis on the other hand has it all wrapped up as far as the user interface is concerned. The humble hyper-link is clicked on 1 x 10X per day where X is greater

than 10. When it comes to vox populi, or the voice of the people, any computer interface is going to fail on the basis of these statistics. No focus group, design team or engineer on the planet can overcome the intimacy that billions of people have developed with clicking on an HTML link. I would guess that Bob Bemer didn't have a focus group on hand to test efficacy. So Google, the future is yours in

be utilitarian, some revolutionary. What goes on underneath the bonnet will be hidden to the majority of users, but first impressions really matter. We all intuitively understand good design – it has that feel about it, an aura, a quality you just cannot put into words. It pulls you into itself, re-enforcing your understanding of the universe yet at the same time challenging you to explore further. It is greater than the sum of its parts. So maybe the demise of Red Flag Software is a mercy killing rather than an assassina-

terms of statistical dominance.

Yet we still have the problem of the UI bling factor – the pretty, touchy feely effect that Apple has embraced and made almost a religion out of. While the hyper-link is cold and efficient, exploding windows, cute animal sounds and great font rendering bring élan to an emotionally sterile environment. MSC has never quite penetrated this US West Coast paradox, yet we see the same trends with those who love their Android O/S and the touch screen. It is the “wow” factor.

At the end of the day, software interfaces need to be just that – an interface. The same rules apply to the design of a car, a cheese grater or a garlic crusher. Some will

tion. If the move to the cloud and thin client is the next revolution, it matters little what that thin client will be, as the forces of mass adoption will dictate how people interact in cyberspace. The O/S will become less and less important, and the user experience and interface will become more so. And that is where the trojan horse of Open Source will dominate – the power behind the throne.

---

### ROB SOMERVILLE

*Rob Somerville has been passionate about technology since his early teens. A keen advocate of open systems since the mid-eighties, he has worked in many corporate sectors including finance, automotive, airlines, government and media in a variety of roles from technical support, system administrator, developer, systems integrator and IT manager. He has moved on from CP/M and nixie tubes but keeps a soldering iron handy just in case.*

# With Every Business a Target for a Security Attack, are Organisations Finally Grasping the Security and Data Protection Nettle or is the Issue Still Being Kicked Into the Long Grass?


I have just had a very busy week. Security flaws were found in a major IT system prior to launch which was duly taken offline and a more secure temporary solution implemented and rolled out in double quick time. Fortunately there was no business or data protection impact, and we even managed to score a pyrrhic victory by getting the vendor to admit that this issue was indeed an issue, and they have gone away to think about solving it. I suspect though that the offending piece of software will ultimately end up as abandon-ware as the cost of really fixing it properly will be so prohibitive that the vendor will be forced to pass the costs on to the customer base, making the project financially unsupportable. Sadly, it was only a matter of time. Our IT department had valiantly raised our heads above the parapet on many occasions about issues with this particular vendor, but due to internal politics it was decided to carry on regardless. Finally the penny dropped, and it looks like a more appropriate technical solution may be rolled out sometime in the future. One for instance that will have a decent API, something that the vendor in question refused to provide as it was not in their commercial interests. They would far prefer to supply a proprietary integration solution at a cost of tens if not hundreds of thousands.

While I am happy that this issue is now being addressed, it is by no means a victory. It wasn't until the weight of evidence was so overwhelming that the decision was taken, and so much pain could have been avoided if the professional opinion of IT had been respected in the first place. The problem comes back to the classic disconnect between IT and management – and the army of departments that want to live in their own little silo with technological autonomy. This is the danger when complex devices and systems are marketed in the same way as block box disposable consumer goods. Nobody wants to think about what goes on under the hood, and those that

support and manage these systems are often regarded more as technicians than engineers.

In reality, the word engineer is derived from the Latin *ingeniare* (“to contrive, devise”) and *ingenium* (“cleverness”). The word technician is a modern construct. To start with, there is a lot of professional jealousy – often on the part of formally qualified engineers – when IT adopts the word “engineer” rather than “technician”. Woe betide the skilled programmer or developer who has not got a technical qualification to their name adopting the title “Software engineer”. This professional snobbery extends through the management layers, often with the mantra “Paper qualifications good – experience alone bad”. The most acclaimed and innovative piece of engineering in human history – the wheel – was invented at the latest between 6500 and 8500 years ago. There is no record of the inventor's gender, but I doubt if they had any professional or educational qualifications to their name.

No, the problem lies in the formalised, metricated, quantified, and qualified society we live in. There is no longer any creative space for the innovator, the idealist, the visionary or common sense unless of course they are willing to work within the strict confines of finance, regulation, management, censorship, or control. That is why whistle-blowers and creatives are in such short supply. If you have the right position (i.e. one with clout), you can apparently defy the laws of the universe – but only for a short while until you are found out. Then the PR mantra of “Lessons learned” and a “One off incident” are wheeled out, unless of course the regulator or the justice system bites and then you are really in trouble. The Information Commissioner's Office (ICO) has fined the charity British Pregnancy Advice Service £200,000 for exposing personal data to a malicious hacker via their outsourced website. While I have a great deal of sympathy for the apparent injustice of a charity being fined for a data protection breach, the disconnect



is obvious. The trustees placed their trust in a third party who had no real loyalty to the organisation other than to provide a website, and knowing the extreme financial pressures placed on charities and the public sector, there would have been a very tight budget. So no room for penetration testing, a code audit or probably even a decent specification that took into account the data protection risks in such a politically charged arena. The BPA management team will have a harsh lesson to learn on

pushing the envelope. IT professionals have no such latitude. Systems are ruthless, almost psychotic in their level of un-forgivenesses. A full stop in a wrong place in a line of code, an unreliable piece of hardware or a badly written specification document can wreak havoc. Never mind deeper logical issues, system complexity, and the hundred and one other pressures that the poor “technician” has to deal with. Good IT people develop a sort of sixth sense over time – call it intuition or whatever – that alerts them to danger. I continually have my leg pulled by colleagues at work because all my servers are backed up daily and every so often I check that the backups are valid. I will not take risks unless I have a plan B and preferably a plan C and D as well. So I go home at night, put my head on the pillow and sleep soundly. What gives me nightmares though is the disconnect between senior management and the technologists – especially where you have a department in the middle that demands their own 3rd party system – and get it. My IT sixth sense knows that the true cost of that system – fully supported, patched and maintained – will be way above the negotiated and signed contract that is eventually agreed upon. So we have IT by committee, built to a price with excellence and worse case – best practice tomorrow. And when the wheel comes off, IT will be will be the first port of call to support a system as after all we are only “technicians” and surely it can’t be that complicated to fix. It is no wonder that in IT departments up and down the land, staff have major difficulty in resisting the urge to display banners above their desk that say “I told you so”. Hopefully the tide is changing. Organisations are beginning to understand. My engineer manager friend (who is convinced I am a technician) bemoans the lack of “engineers” and freely admits that this is due to lack of candidates willing to work for peanuts. Yes, the downward pressure on salaries is a short term problem, but the bigger long term problem is the cultural divide. Maybe if a few CEO’s and CTO’s sat down with their IT departments over a beer there would be less potential room for corporate embarrassment.

### ROB SOMERVILLE

*Rob Somerville has been passionate about technology since his early teens. A keen advocate of open systems since the mid-eighties, he has worked in many corporate sectors including finance, automotive, airlines, government and media in a variety of roles from technical support, system administrator, developer, systems integrator and IT manager. He has moved on from CP/M and nixie tubes but keeps a soldering iron handy just in case.*

# With the Recent Announcement of the Widespread Heartbleed SSL Vulnerability is it Time to Reconsider who the Troublemakers Really are?

Unless you have been away from the newspapers, television or the internet for some time, the widespread media coverage (and to some degree panic) of this particular coding error in the OpenSSL library will not have escaped your attention. Due to a fairly trivial coding oversight, an attacker can compromise any server running SSL and extract X509 keys, cookie data, usernames, passwords or even potentially documents. This affects OpenSSL from versions 1.0.1 through to 1.0.1f – a vulnerability window of 2 years in the wild.

I'll be the first to admit then that my optimism in last month's column about security matters improving was probably premature taking into account this latest announcement. I think in the future I will return to the cynical position that the only secure computer is one encased in concrete and dumped in the bottom of the Western Pacific. What is more disturbing is the announcement by Bloomberg News [1] that the NSA was aware of this exploit for two years and did not alert the software security community or OpenSSL. The NSA naturally denied this, but to paraphrase the immortal words of Mandy Rice-Davies who was embroiled in the UK Porfumo spy scandal in the 1960's – "They would, wouldn't they?"

So let us look at the anatomy of a bug, particularly insidious ones like Heartbleed. To start with, the more complex a piece of software, the greater the chances there will be errors in it. If more than one programmer is working on a project, the greater the possibility that errors will accumulate. I say "Aluminium" where as State side, it is "Aluminum". One coder will use a for .. each loop, another will use a do ... while loop. Differences in writing style, design and logic will always plague large projects, even with strict controls in place, as people have a natural or cultural approach to coding these syntactical and logical errors will creep in. And that is before we even get down to the nitty-gritty of genuine bugs, where code has been tested thoroughly and

found to be fit for purpose. The infamous Therac-25 radiation therapy bug that killed patients undergoing radiotherapy would only arise when the operator pressed an obscure sequence of keys. The other lesson that was not learned is that previous versions of the software were reused and modified. Unfortunately, the earlier version was dependent on a hardware interlock preventing the fatal scenario. In later versions, the software acted as the interlock, and as the previous fail-safe masked the true nature of the bug mistakes were made.

And so it is today with the programmers' dependence on libraries. Best practice always says "Don't reinvent the wheel" yet how much confidence can a developer have on any library? Human beings make errors, and even the best programming team in the world cannot produce 100% reliable, bug free code that will work flawlessly under every circumstance. That is why the Open Source movement is so critical in these days of technological complexity – the community is much larger than any corporate division and with peer review the chances of problems coming to light sooner are much



greater. From a security and code review perspective, Openness is good, Opacity is bad. That is why, if true, the failure of the NSA to notify the developers concerning Heartbleed is so morally and ethically repugnant. While I fully appreciate the difficulty that is the ethical minefield of National Security, to me – naively I know – behaving in this way seems a total betrayal of why the agency is there in the first place. A cynical colleague once suggested that a lot of viruses and malware were designed by the Anti-virus software manufacturers themselves to keep their businesses viable. He may have been closer to the truth than he thought.

So who are the real troublemakers? If a tree falls in a forest and there is no-one there to observe it does it make a sound? Without an attack or extensive research by the security community, a lot of these errors will remain hidden. All software has bugs and vulnerabilities. Period. From the O/S right through to the user interface, the thread of error runs. While some are more diligent than others in writing quality systems, we will not reach perfection in this lifetime no matter how hard we try. The developer using a third party library trusts the third party. The

end user trusts the IT department to source the best software for the purpose at hand. The customer trusts the company or organisation. Like banking, the IT industry is built upon layers of trust, and where this is betrayed, confidence is reduced. Unlike banking, the industry is still young and developing, so there is hope that we will grow and mature accordingly. However, our hands are tied by the disconnect between the technologists, black hat hackers and the establishment. There are

stringent laws in place with punitive sentences for those that breach the computer misuse act. If I were to probe a third party SSL server without the owners' permission to definitively prove whether or not it was vulnerable to Heartbleed I could potentially leave myself open to prosecution in the UK, and no doubt the USA as well. That seems fair until you realise that > 66% of the servers out there are probably vulnerable to this bug. Will all these sys-admins patch their code? What about organisations that are undergoing fiscal cuts and do not have the technical resources? To deal with Heartbleed will take a lot of resources and ideally the internet as a community should

be the one to deal with it by identifying this silent and pernicious weakness and lending a helping hand. No wonder some people on forums are saying "Stay off the Internet". If all you have is someone's word, without empirical evidence, it is a lot to ask when your credit card or personal details are at stake.

The black hats on the other hand will be having a field day. The call has already gone out to build an army of Heartbleed honey traps, but more troubling is the potential data loss that may have quietly occurred unseen in the previous two years. There are known knowns. There are known unknowns. There are unknown unknowns. If I was a Black hat, and discovered such a vulnerability, I would make sure I kept very quiet indeed and make hay while the sun shines. Now that the attack is out in the open, all bets are off. It will be a straight race between the Black and White hats with those that are not technologically aware no doubt accidentally tripping both sides up from time to time.

As an industry, we need to grasp the nettle of ethical disclosure, and help each other out but unfortunately this will be a tough call. Walking home one night, I saw a car parked outside my house with the driver's door unlocked and the keys in the ignition. I didn't recognise the car, and being an area renowned for joy-riding and car theft, I checked the car to see if I could find any clue to the ownership details. Finding none, I locked the car and phoned the police to say I had the keys, and would they like me to drop them off at the police station? Thanking me for my community spirit, they got in touch with the owner. Unfortunately, it was my next door neighbour, who was fixing the car for a friend and was duly reprimanded by the owner for his carelessness. I didn't even get a thank you – just a very gruff "Keys" and an angry glare for my efforts when he knocked on my door late that night. As the old saying goes, no good deed ever goes unpunished.

## References

- <http://www.bloomberg.com/news/2014-04-11/nsa-said-to-have-used-heartbleed-bug-exposing-consumers.html>
- <http://www.theguardian.com/technology/2014/apr/12/us-government-nsa-denies-aware-heartbleed-internet-bug>

## ROB SOMERVILLE

*Rob Somerville has been passionate about technology since his early teens. A keen advocate of open systems since the mid-eighties, he has worked in many corporate sectors including finance, automotive, airlines, government and media in a variety of roles from technical support, system administrator, developer, systems integrator and IT manager. He has moved on from CP/M and nixie tubes but keeps a soldering iron handy just in case.*

# In a Surprise Decision, Europe's Top Court has Ruled That Google can be Forced to Erase Links to Content About Individuals. Is History Repeating Itself Once Again?

**T**hose who cannot remember the past are condemned to repeat it, or so said the philosopher George Santayana. In a previous article I had a good rant on how the UK Conservative coalition – during an unexpected but not unsurprising period of hypocrisy – requested the removal of all of the parties' election promises from the Internet while at the same time supported the banning of over 100K keywords related to child pornography. To reiterate, I find both actions morally repulsive, because a) the former should be a permanent matter of public record and b) the latter is as useful as a chocolate teapot in defending children from the evil of pedophile abuse. For those that are still listening, generally, technology is not best served by committees, lawyers, judges, politicians or indeed governments as they just "don't get it". That is not to say that there are not IT savvy individuals in these sectors – there are – but generally their voices are drowned out by the herd of the ignorant.

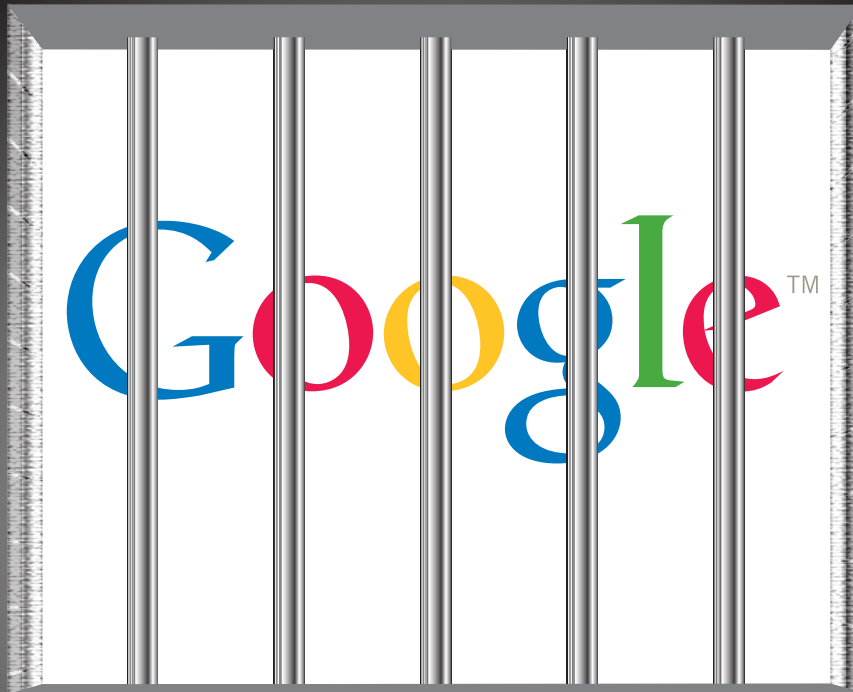
Fairly soon they will take me away in a wooden box and bury me in the ground. Whether that be 5 years, 10 years or 25 years from now matters not one whit, but I will go to my grave ranting that what is happening to the Internet and the World Wide Web today is identical to what happened during the time in history when books first became the "new media". Ergo, the establishment got pretty worked up about the peasants finding out "esoteric knowledge" and the church (in this case the Roman Catholic Church) stepped in to be "God's censor". The fact that this knowledge was the Protestant bible (and there are those who argue the protestants didn't go far enough) is neither here nor there – the principle remains that an element of the establishment was not happy and did everything in its power to censure, burn, character assassinate and torture those on the side of an alternative view, revelation and freedom of speech.

I am not a great defender of corporate culture – particularly corruption and ethical misdeeds, and it is rare that I will be found taking the side of Google – the new Microsoft. But in this case, they have a point. If Google is to be taken seriously and if you are to look at today's younger generation, Google is indeed the font of all wisdom – how can redacting the past elicit credibility? And herein lies the problem – is Internet content a pastiche, a snapshot of history or just a temporary communication medium without value? As the old saying goes, a verbal contract is not worth the paper it is written on. After all, Google is the world's biggest log-file.

Where I come from, a man's word is his bond, and I expect the same from my computer. A trusted and proven friend will have more credibility than a stranger, likewise there are a number of websites I trust. While Google is still fighting the blowback from its original ethical stance of "do no evil" in the UK due to ethical issues over tax, it is still the world's leading search engine. There are those that can add to this faux pas, and no doubt the underbelly of Google will be found to be as grubby as any modern corporation. However, that should not divert us from this ruling that gives pedophiles, criminals, corporates and other undesirables the ability to put a gun to the head of the messenger and legally demand – like a cat burying its feces in the ground – that all trace of embarrassment should be removed. Like cat shit, this stinks.

Of course, like any publisher or voice of authority, there needs to be a balance. And that balance needs to be firmly placed with those who write and publish on the Internet. Never has the need for ethics, oversight and just sheer common sense been more required than in these days of Facebook, Twitter and the Blog. The Duke of Wellington said "Publish and be damned", but that was more akin to the Gaelic shrug of indifference than





to the current understanding – that publishers must take responsibility for what is printed (albeit in electronic format) – is a good ethical principle.

Forcing Google to remove links is akin to breaking into a library and removing the Dewey index card for whatever book offends the reader in a library. The content is still there, but hey ho, situation ethics wins so my only hope is that the Streisand effect will kick in and give those that choose to go down this route a run for their money.

Let's be clear though, a lie goes halfway round the world before the truth has got its boots on. Everyone – Publishers, Google and ISP's have a responsibility to ensure that the Internet is a truthful and valid source of information. And here we really start to open a very large can of worms – for throughout the ages the powers that be (or the aliens, take your pick) have sought to corrupt, debase, and change the very fine thread of truth that characterizes a particular scenario. Propaganda, spin, advertising, statistics – all of these have a huge impact on human consciousness. And the Internet is rife with them all. Again it goes back to the publishers, but maybe we need some discipline on the the good old Interweb. Where do we draw the line between entertainment, opinion, experience, knowledge and truth?

I'd love to be able to come up with a definitive answer, but like the human condition, the answer is a bit more

complex. Google, like the Internet, is just a mirror placed at the face of humanity. Those that choose to scrape the silver coating off the back so that a true reflection will not be seen will so crudely distort the image that the cries of "foul" will be louder than their misdeeds, and thereby attract more attention to themselves. That is, of course, if Google has the courage to display the link with the words "We have been asked to remove this link because ...." Otherwise, we will have an interesting scenario whereby Google can comply with the Digital Millennium Copyright Act by leaving a link while erasing more interesting material without a trace.

I really hope Google is as enraged about this as they are pretending to be. Bowing down to the DMCA was bad enough but to crumple on this will take "Do no evil" to the new low of "Do nothing".

---

### ROB SOMERVILLE

*Rob Somerville has been passionate about technology since his early teens. A keen advocate of open systems since the mid-eighties, he has worked in many corporate sectors including finance, automotive, airlines, government and media in a variety of roles from technical support, system administrator, developer, systems integrator and IT manager. He has moved on from CP/M and nixie tubes but keeps a soldering iron handy just in case.*

# A recent poster on <http://www.theregister.co.uk> lamented that with all the recent security failures and the increase of patching, IT is not fun any more. Are we facing a new dark period in the technology sector?

I am a grey-beard when it comes to IT – both literally and metaphorically. Having cut my teeth on the IBM XT, I have seen just about every cycle that hits the technology sector, from euphoric optimism to the sky is falling. I have witnessed IT slide from a hallowed profession in the eyes of management to “just another resource” and the widespread adoption of technology in areas of our lives we would have never envisaged 10 or 20 years ago. Trends and cycles come and go, but there is something different in the wind this time around.

Fortune 500 companies are bringing resources back in house, as major employers face a quality and recruitment crisis. Globalisation forced down salaries, and the opportunistic bean-counters – who appreciated the cost of everything and the value of nothing – fed the management culture with the mantra “We can cut costs and improve productivity”. *Et voila*, we have the current scenario where employers are desperate for staff with enthusiasm, who think outside the box and are willing to go that extra mile to solve complex problems. I have been persistently canvassed by a close friend who works in the Nuclear sector to join his organization on the basis that they cannot recruit staff who are willing or able to think outside the artificial standard that HR requires – e.g. a degree. Sometimes, metrics just don't work.

Like all specialized areas, you can tell a skilled practitioner not by the paperwork, or the clothes, nor by age or gender but by the attitude. How they think. The way they see problems, what they see as important as values and what is ephemeral. Unfortunately the culture in the West has gone for the “Measurement and control” route, rather than a more creative solution. Don't get me wrong – discipline and management are essential – especially when it comes to large organizations and systems, but the culture has swung too much towards the fascist, and the chickens are coming home to roost. All I hear in the media (certainly in the UK) is that we have a skills shortage, but it is not surprising while we have

a scenario where commitment and true value are not rewarded over paperwork, audits and internal politics and culture.

My employer has recently recruited a new project manager, who for the first time in the long queue of his predecessors, has actually commented on my performance. To some, his comments would be offensive, but to me personally, I take it as a badge of honor. To quote the immortal words of Tommy Cooper, the apocryphal British comedian and magician, “Let me tell you a story”.

I was once employed by a famous British museum, and my role was to design and maintain electronic exhibits. I loved my job, and I would still be there today if the salary was enough to keep a family, but reality being what it was in the 1980's it was touch and go even as a bachelor. That said, one day a department had a serious problem with their CP/M based system and I was asked to have a look at it. Discovering that it had a hard disk failure, I informed the manager concerned what they needed to inform the supplier, and in the process saved them engineering time diagnosing the problem and hopefully shaved some money off the final repair bill. Sadly, this was not welcomed, as my head of department had a pathological hatred of the department I assisted. I was consequently marked down on my annual report as “Too enthusiastic for the job”.

So lets get back to our PM, and for the sake of this article, let's call him Dave. Dave has all the credentials, and as PM's go he is a decent sort – I actually have time for the guy. He even mentioned the other day that (to paraphrase) “He will need to channel my enthusiasm”. Now, taking into account the natural animosity that resides between IT and PM's in general to either default to a) Bow down to their methodologies while paying lip service and let them find out the hard way – generally just before forced change of employment or b) Ignoring them entirely, I decided to engage. I could have sat him in front of a BSD server and asked him to manage it, or asked him



to solve the particularly tricky stability solution we have with our web-server. But I had compassion. I talked about the organizational culture, and how I would not do his job for all the tea in china.

Simply put, Dave understood the battle that all IT departments and their staff have – the problem of breaking the cycle of disconnect. Ironically, like HR, IT are now relegated to a process and function, something that can be measured by performance, reliability and uptime. Unfortunately, hackers and the dark side do not respect these metrics and will do everything to exploit this disconnect on every level possible. Some would say the current system works in their favor. It takes a lot more than organization to run an organization. Synergy, commitment and (dare I say it, Dave) enthusiasm are vital.

I'll be the first to admit, I am like a golden retriever – throw the ball and I'll fetch. I don't have time for politics, petty squabbles, or inter-departmental rivalries. I want to demonstrate my skills, bring "magic" to the end user, and ultimately the customer. I am goal orientated. Yet, for so long, IT has not been allowed to manage itself, and have accountability where it matters – at the board level. Yet, as the heart of any organization, like Dave, we are deeply misunderstood.

So let's put this scenario in perspective. A major communications company spends obscene amounts of mon-

ey relocating staff on a regular basis so that they can have a window seat. I doubt if Dave would recommend this, but it is a rather good analogy as to why we are in the mess we are in, and why it will get worse. Instead of confronting the elephant in the room, we spray deodorant, place proximity sensors around the perimeter, and from a cultural perspective deny the existence of the aforementioned mammal.

From a security perspective, all bets are off. We have moved from a battlefield of munitions to software, vulnerabilities, and Intel. The first line of defense will be the fire-wall, and those that support and man it. With management's track record over the past 20 years will we have an army of amazons to repel all boarders or those that have had all the stuffing systemically knocked out of them? Enthusiasm and fun aside, there is no test for a hero.

---

## ROB SOMERVILLE

*Rob Somerville has been passionate about technology since his early teens. A keen advocate of open systems since the mid-eighties, he has worked in many corporate sectors including finance, automotive, airlines, government and media in a variety of roles from technical support, system administrator, developer, systems integrator and IT manager. He has moved on from CP/M and nixie tubes but keeps a soldering iron handy just in case.*

# While it cannot be disputed that the World Wide Web and the Internet has helped in speeding up the advancement of globalization in eroding national barriers – is there a down side to mass connectivity?

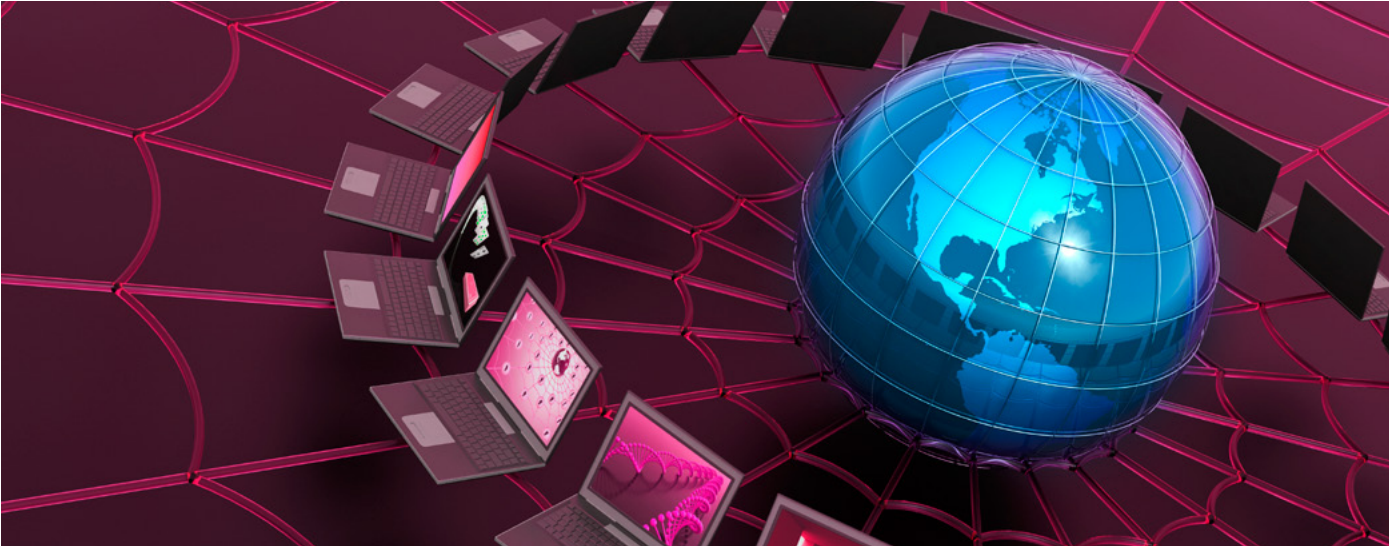
I have just finished reading an excellent book by *Alex Perry* – the award winning Time journalist – entitled “Falling off the edge, Globalization, World Peace and other lies”. Therein are contained some frightening statistics, not just concerning the inherent national angst and violence that arise when sudden change is imposed upon a country. Take India for instance, at current levels of growth it will require more than 100 years for the nation to reach parity with living standards in the West. During the Iraq war, more journalists were killed than during the whole of the Vietnam war. While the author makes clear his distaste for the globalization agenda from the viewpoint of a hardened war correspondent, the parallels between the socio-economic-political and technological universes could not be less contrasting.

While the crux of the anti-globalization argument rests on inequality – the “haves” versus the “have not’s”, the resource rich versus the resource poor, the strong against the weak – technology has almost always been considered the great leveller. And with the similar ethical passion as the politician, banker or plutocrat, the argument has always been that wealth trickles down – be that financial wealth or educational knowledge and skill. It is however becoming more clear in these recent years of austerity that this model is broken – as the gap between rich and poor is widening not decreasing. And so it is with technology. Apart from the few who really want to get their hands dirty, the majority of people are happy with their Facebook, Twitter, Email and website access until of course when the communications go down or a virus attacks in which case all hell breaks loose. Our Internet connection here has been very unreliable over the past few months. Mainly I suspect this is happening due to the roll-out of Fiber in the area – at one point I was experiencing the lightning fast connection speed of 100Kbps and all without the comforting sound of a pair of modems handshaking.

My teenage daughter was climbing the walls, and life was definitely more – not less stressful.

Now, I could be accused of over dramatization here – after all, wars, rebellions and uprisings kill people – a lifeless Ipad or PC will rarely be cited as the cause of death on a coroner’s certificate. But dig beneath the surface, and the same subtle dynamic is at play – you must be part of the crowd or else you are an outsider. Join the technological arms race or be flattened by the opposition. Sup at the communal bowl of the Internet of Things (IoT). And then you may pick up some nasty diseases while you are at it. The problem is not the connectivity; it is the uncharted territory that goes with it. What is sauce for the goose is sauce for the gander and the old establishment is reeling as the openness of new media is exposing their weaknesses quicker than the traditional channels ever could. Politicians and legislators are struggling to keep hold as the criminal and terrorist move from the more visceral bank robberies and bombings to fraud and electronic infrastructure attacks. The definition of property is being redefined by mega-corporations, and personal data became public knowledge years ago. And here lies the rub – while not explicitly stated by Alex Parry, you can almost touch the intellectual exasperation on every page of his book – where has the ethical order gone? Why are we descending into chaos?

It would be easy then, to take the simplistic view and say the Internet is broken and try and regain it. This seems to be the current philosophy amongst the powers that are existing and thankfully we are not yet at the stage where we have UN peace-keepers patrolling the World Wide Web. However, the insidious creep of government vampiring our network traffic and communications is continuously unabated at the same time that Internet censorship is on the rise. As I have stated many times, politicians and lawyers are best kept as far away from regulating technology as



possible as they rarely appreciate the subtleties of robust engineering or human ingenuity. What is more troubling is that we can expect the same global solutions to the global problems as we have had over the past hundred years – in other words sweet nothing other than to make the problem much worse in the long term. The technological age was meant to bring in more free time, a paperless office, free electricity and a better quality of life for everyone. For a few, this is the case, but the majority of the world remains poor, hungry and dispossessed. We can send a man to the moon but can't manage to get clean drinking water to the 780 million people who need it. And where do the global leaders house their outsourcing operations? Where it is cheap – like India of course.

In the late 80's and early 90's, there was a great trend for multinationals to be ethically led. I had the pleasure of working with two visionaries – *Michael Kidron* and *Bela Hatvany* – in a small tech start-up that monitored the ethical behavior of multinationals and blue chips. Sadly, it was ahead of its time and didn't make the grade in the harsh world of pre-internet electronic publishing. Sites like *Wikileaks* today have global reach, but the pace of change is too slow and in the arms race a small organization has no traction with a huge PR machine – especially if it has access to other forms of media or worse to be the ear of a government. That is why it is so critical that the Internet remains a pure voice for all. This curse of “managing expectations” has penetrated through corporate website forums, blogs and message feeds to the extent that PR companies are now advertising on commercial radio offering to manage your reputation on the web. Software tools are used to monitor Twitter and Facebook in the guise of customer service, but you can bet that the real motive behind this is to silence any real criticism.

Nature abhors a vacuum, and as we have allowed commercial interests to dominate the infrastructure of the Internet, now so shall they dominate the ethical landscape as well? And as it is with the global erosion of sovereignty, so will it be with our meta-data? The majority will go along with the agenda, not realizing that the first call of any reputable recruiter or law enforcement officer will get their Facebook pages. It is very easy to click in haste and repent at leisure.

And far away from the suggestion that we need an Internet policeman, we do however need stronger ethics and vision for the Internet. Not just on the corporate level, but for the 70% who are not online and cannot speak for themselves. From where I stand, that is the only positive point I can see – a bunch of connected, networked individuals who make a stand and say with one voice “This is not right”. If the Internet loses its edginess, and becomes just another media-barons paradise on a global scale, we really will have lost any voice as the sticky ocean of mediocrity, alternative agenda, doublespeak and compliance smothers any dissenting opinion. *Mike Kidron* and *Bela Hatvany* had it right 30 years ago – *the deeds of large corporates, governments and institutions need to be truly independent-monitoring – and they need to be held to account.*

---

## ROB SOMERVILLE

*Rob Somerville has been passionate about technology since his early teens. A keen advocate of open systems since the mid-eighties, he has worked in many corporate sectors including finance, automotive, airlines, government and media in a variety of roles from technical support, system administrator, developer, systems integrator and IT manager. He has moved on from CP/M and nixie tubes but keeps a soldering iron handy just in case.*

## Over twenty years ago, Mitchell Kapor, the founder and former C.E.O. of Lotus Development Corporation stated, “The question of what to do about Microsoft is going to be a central public policy issue for the next 20 years. Policy makers don’t understand the real character of Microsoft yet”. Has government and industry smelled the coffee yet?

I am writing this column on the last day of my annual holiday and to be perfectly honest, I am not looking forward to going back in the trenches again. Just before going on leave, our organisation had an outbreak of the Cryptowall virus, and while we have managed to contain this professionally, in one day alone our external firewall rejected over 5,000 infected attachments. To add insult to injury, my broadband line at home has been playing up since late last year culminating in spasms of slow and intermittent connectivity and no land-line, sometimes extending to periods of over 10 days. In a final sop to the front line technical support desk, I have relocated all my IT kit downstairs next to the master telephone socket to “prove” the fact that it is not our internal house wiring – much to the chagrin of my long suffering wife. The final straw came last Friday, when after 10 hours of downtime I phoned my ISP for the umpteenth time just for the ADSL to come back up again while being held in the telephone queue. Now to give my ISP their due, they have always been extremely apologetic, helpful and efficient – but the core problem has lain with the infrastructure provider. I have been promised an engineer visit on Friday so hopefully we will get to the root of the problem, but I have my reservations. Unless the line decides to exhibit a fault during the tests, the usual cat and mouse game of trying to trace and isolate an intermittent fault will continue *ad nauseum*.

And so be it with the scammers who are currently behind the current wave of encryption malware. Having examined the offending exe’s with a hex editor, part of the payload embeds the path of the infected user directory in the exe itself thereby circumventing any detection via checksum, which is a common method used by anti-virus software. So from the hacker perspective for every machine infected, you potentially have a zero-day exploit at hand to mail out to another tranche of victims. With mass-mailer malware regularly included in the latest generation of viruses, this is a pernicious form of attack. Unless your anti-virus software is set to paranoid mode, there is a good chance something nasty will get past. And of course, this does not prevent users from accidentally or foolishly clicking and opening an infected attachment disregarding any warning messages. Or in the case of a particularly demented user I once encountered, turning off anti-virus software altogether as it slowed down his PC.

As I have stated on many occasions, trying to get Law Enforcement (in the UK at least) to take an interest in this is virtually impossible, unless of course you have been defrauded in which case you are urged to contact them. With small businesses becoming victims it is not unheard of for people to pay the scammers to get the encryption codes back, in which case if the decryption process is successful it results in a very interesting paradox – the scammers’ reputation rises if they honour their word. In theory,

they have fulfilled contract law, which is an astute move as the penalties under civil law can be greater than under criminal law and the burden of proof is based on the balance of probabilities rather than beyond all reasonable doubt. So proving fraud if you make payment potentially could be difficult. The fact that this whole distasteful scenario takes place across international boundaries with different legal systems over an encrypted network and you can understand why the police are so slow to act. So where should we point the finger?

If we were to design doors and windows for housing that let rain and wind in, nobody would buy them. Unless of course I was a virtual monopoly, and then there would be great outcry to the policy makers about “Fitness for purpose”. Another better supplier would be appointed and I would in reality face bankruptcy. Unfortunately, Microsoft has had all the benefits of a trojan horse, and decades have passed so it is now in the magical alternative universe of being “Too big to fail”. Vested interest has firmly cemented Microsoft’s feet under the corporate and domestic table. Likewise with the telcos – as an individual I have a snowball in hell’s chance of suing for breach of contract due to lack of service provision; all the small print in the Service Level Agreements has seen to that. So as the “little man” in reality I don’t have much choice as far as infrastructure is concerned apart from maybe moving houses.

50 years ago, the British Prime Minister Harold Wilson called for Britain to be forged in the “white heat” of a technological and scientific revolution. We have got that all right – but it is the anarchists rather than the citizens that are driving change. Software security vendors are calling for a form of Internet Identification – but as any intelligent person knows this will play into the hands of the fraudsters – rather than stealing passports and drivers’ licences, Internet User ID’s will be the theft of choice for the criminal, all the while their co-conspirator Microsoft will plead innocence. If you think I am being harsh, in law Microsoft’s role could be considered “Aiding and abetting” under English law, and “Accessory before the fact” under an American jurisdiction.

We have reached the point of critical mass, the tipping point where the perfect storm of greed and convenience has won over strong engineering design principles. Microsoft is not the only culprit here; Adobe (and no doubt many others) have embedded themselves so deeply inside the operating system that they are virtually inseparable. Having understood the issue of regular cookies, a well educated computer-literate friend of mine was shocked when I explained to him the scope and use of Flash cookies. And people wonder why the concepts of encryption, pri-

vacy and security are gaining traction and publicity of late. For too long the corporates have ignored these principles and now the chickens are coming home to roost. The Internet and use of Internet connected devices is now so ingrained and essential to smooth running of a modern society that it is on par with the mission-critical status of the electrical, water, fuel, and food chains. If any of these services break down, optimistically you have a window of 7 days maximum before civil unrest takes over. Here in the UK, benefit reforms are forcing claimants to register and apply for jobs online. And yet we do not have a secure and reliable technology platform other than those based on Open Source, and it could be argued (rightly so) that the only reason that it does not fall foul of the criminals is due to lack of consumer footprint. I hope and pray that it does not happen, but at the current level of attack it will not be long before something major collapses – whether this be the widespread compromise of a bank, government agency, media outlet or health provider *et al.* It is already happening piecemeal on an individual basis, as happened recently with the failure of the Adobe Creative Cloud (which was not security related) unlike the theft of the encrypted credit card details for their 38 million subscribers. All it will take is sloppy management and a particularly vicious payload. It matters not the reason – financial exploitation, sheer will-full destructiveness or technological warfare on the part of a hostile country – the damage will have been done.

The biggest virus of all, a colleague wryly commented *is* the Microsoft operating system. Once the penny drops in the marketplace that current software and infrastructure solutions are no longer sufficient to keep us or our data safe and that we have a global single point of failure – technology – the future for MSC and other culprits will be bleak. The Emperors’ clothes will be seen for what they are, and both the anger and the response of the consumer will be unprecedented. We have until then to address this by legislation, law enforcement, innovation and design unless we want Information Technology as an industry to be relegated to the ethical trash can like politicians, estate agents, lawyers and used car salesmen.

---

## ROB SOMERVILLE

*Rob Somerville has been passionate about technology since his early teens. A keen advocate of open systems since the mid-eighties, he has worked in many corporate sectors including finance, automotive, airlines, government and media in a variety of roles from technical support, system administrator, developer, systems integrator and IT manager. He has moved on from CP/M and nixie tubes but keeps a soldering iron handy just in case.*

# The UK government is planning to put trolls in jail for up to two years. Is this a sensible approach in containing the darker side of human nature?

**T**rolling, the deliberate posting of offensive or controversial comments via Forums, Facebook, Twitter etc. is not a new phenomena on the big nasty inter-web. The phrase “Don’t feed the trolls” (DFTT) has been around as long as I remember – going back to the 1200 baud modem and bulletin boards in fact. But what is the psychology behind this desperate and compulsive act? Apart from the nastier incidents like threats, bullying and the tragic case where a grieving family was sent pictures of their deceased daughter after an accident, most people would agree that trolls are either immature, borderline psychopaths and sociopaths, bad mannered, deeply insecure or a combination of all of these characteristics. The nastier breed are just evil. But is this sufficient reason to newly criminalise behaviour that traditionally was dealt as a civil matter with damages being awarded? While physical abuse has always been dealt with under criminal law, character assassination, defamation, slander and libel are covered by civil law.

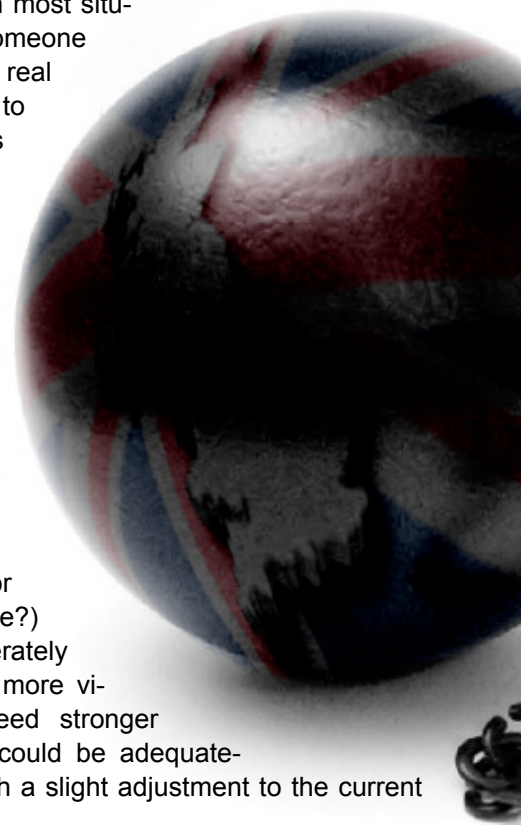
Studies have shown that individuals engage very differently online than in “real life” or face to face situations. The current debate about online ethics and behaviour questions whether online activity is closer to reality than fantasy – e.g. you should not engage in behaviour online than you would not do in normal physical life. While I agree with this statement up to a point, the online boundaries are blurred between reality and fantasy. What is appropriate in a online game session, the sports field or the workplace are very different standards indeed. Human beings adapt to their environment, and the surrealism of the Internet does not help us easily identify where the moral boundaries are. I would go as far as saying that peoples personality subtly changes when they go online, very much like the quiet man becomes a speed freak or road rage instigator when behind the wheel of a car.

Anonymity is a two edged sword – from a psychological standpoint people are quickly dehumanised by it, so it is easy to rationalise that there is not a flesh and blood person at the end of that Twitter account or whatever.

That is the real problem with the troll – while their actions may be considered sport, a bit of leg pulling, or based on getting a rise out of people reactions, they probably don’t care about the recipients feelings, but if they do it is a much more pernicious attack – something akin to a damaged child pulling the wings off flies or torturing cats. These are the true psychopath trolls rather than the less malevolent irritants.

So what can we do about trolling? The old adage “Don’t feed the trolls” is probably adequate in most situations. After all, if someone is pulling your leg in real life you would tend to ignore them unless you wanted to engage in the joke. You might even deliver a swift verbal rebuke, but that just demonstrates that you have taken the bait. A Zen like calm is the best approach as it starves the lesser troll of the oxygen (or is it sulphur dioxide?) that they so desperately need. However, the more vicious variety do need stronger sanctions, and this could be adequately covered in law with a slight adjustment to the current stalking laws.

This route however, completely misses the point about network abuse. There are many facets of this – scamming, hacking, phishing, spamming and of course trolling. What we really need is a modification and strength-





ening of the Malicious Communications Act to include the former 4 actions. Ironically, the act currently covers trolling. To quote: 'The Malicious Communications Act 1988 deals with the sending to another of any article which is indecent or grossly offensive, or which conveys a threat, or which is false, provided there is an intent to cause distress or anxiety to the recipient. The offence covers letters, writing of all descriptions, electronic communications, photographs and other images in a material form, tape recordings, films and video recordings.' So in regards to trolling we have the situation (like the phone hacking scandal) where legislation already exists but is not enforced. The political solution to this? Write up another law.

To me, this appears as a typical political knee-jerk reaction while at the same time ignoring the bigger picture. While worse case a vicious troll may drive an individual to suicide (and there is no excuse for the full weight of the law not to be exercised in such instances), in the majority of cases all we have is hurt feelings and a few blows to our pride. The other four forms of lowlife cause much more damage both financially and to reputations. Pity the poor student who has his dissertation permanently encrypted by Cryptowall or a business that has its bank account emptied and livelihoods are destroyed. We seem to have lost the plot where political correctness and hate crime take priority over the nastier network crimes, especially taking into account the sheer

scale of the problem. You might encounter a few trolls per week, but the other forms of abuse are legion.

So it looks like once again the powers that be are disconnected from the reality of the Internet. Two years is a long time to spend in prison for a wind up, and the cost to John Q Taxpayer (and society) is large. Prosecution and police costs are estimated to be £65K with the annual cost of keeping a prisoner in jail £40K. For a maximum sentence, that would cost £145K. Compare that with the cost of a civil action to bankrupt a troll, and depending on their circumstances, the possibility that the troll can repay their victim in cold hard cash and I know which judicial option my wallet prefers. In this time of austerity, we need to prioritise – cut our cloth according to what we have. To create new law at great cost while ignoring bigger issues and at the same time not using the laws we have at our disposal is wasteful, and ethically more offensive than the problem it is trying to address.

---

### ROB SOMERVILLE

*Rob Somerville has been passionate about technology since his early teens. A keen advocate of open systems since the mid-eighties, he has worked in many corporate sectors including finance, automotive, airlines, government and media in a variety of roles from technical support, system administrator, developer, systems integrator and IT manager. He has moved on from CP/M and nixie tubes but keeps a soldering iron handy just in case.*

## Is There a Difference Between Geeks and Nerds?

Forget the Internet wars about vi versus Emacs or Windows versus Linux. Burr Settles has analysed the language of 2.6 million tweets to attempt to answer the contentious question “Is there a difference between Geeks and Nerds?” Let the debate begin.

**H**aving read Burr Settles analysis of the data, watched a number of video commentaries and consumed quite a few articles on the subject, my personal rating is very probably “Gerd”, a mixture of the two. Whereas Nerd is always used as a derogatory term, Geek has a trendier, more metro connotation although personally I still strongly dislike both terms. As an unashamed, in-your-face Gerd I would like to bring some peace and unity to both camps – we share more than our critics would like to admit.

One word I have continually been described as throughout my life is “Deep”. I suspect that term has been applied

examine our commonalities in light of the social majority, rather than bring division – after all, society at large is rather wary of us, hence the pigeon-holing, name calling, and the tag “Being different”. Fear and insecurity is a very strong motivator in the hive mind.

So let’s get back to Deep. My wife has accused me of it, some of colleagues at work have, and very few friends who know me well would tend to describe me any other way. My immediate retort to this is “Define what you mean by deep?” – which in a paradoxically, holistic way not only challenges the person making the assertion, but also answers the question. Gerds refuse to take things at

# GEEKS VERSUS NERDS

to both Geeks and Nerds in equal measure, so I am going to tentatively suggest that we generally have much more in common than we have differences, so rather than type Geeks and Nerds throughout this article, I will use the collective term “Gerd” from now on. Of course, individuals will rate differently on this spectrum, but I want to

face value, always scratching below the surface. Some are content with empirical evidence, some are less satisfied with classical definitions but the resounding trait is to ask questions and search for answers – and quite often questions that are taboo, impolite, or just off the scale. The point is that we have learned early on in life

that most non-gerds tend to live very different lives than we do, one of the major traits being that we live in our heads. While we really do enjoy social interaction, it has got to be based on quality and interchange, rather than superficial social convention and a pretend mask of civilisation. I recently shocked a colleague at work who asked [in social niceties mode] “How are you Rob?” and got the blunt but honest [totally fed up with BS mode] “Rather p\*ss\*d off” reply. I did apologise, but it goes to illustrate why Gerds are classed as socially inept. I should have just smiled, said “Oh so-so” and not revealed my true feelings, but society dictates (at least on this island) that you wear your heart on your sleeve at your peril, stiff upper lip and all that. To me, that smacks of duplicity, if you don’t genuinely want to know where someone is at, don’t ask them. Sure, talk about the weather, the price of fish – anything – but please don’t place me in position where I have to effectively lie to you as it makes me feel very uncomfortable. On the scale of 1-10 of cardinal sins, our social interaction “sleights of hand” may be insignificant, but they are cumulative. No wonder we live in a society where the culture is so superficial, true education and wisdom shunned, and people feel disconnected and isolated. Most of the time I join my fellow conspirators and “play the game” but it does nothing but reinforce my belief that the majority of people (outside of the Gerd community) walk to the beat of a different drum.

I believe that all Gerds feel that their value systems have been betrayed at sometime in their life. Maybe it was totally believing in Santa Claus and discovering you were – whilst not deliberately – effectively lied to (my first personal recollection of worldview shock) or maybe it was just being clever and different in an amorphous peer group. With large ears, thick spectacles, and a comprehensive vocabulary at school I was obvious Gerd material. The favourite insult thrown in my direction was “You swallowed a dictionary?” (My 14 year old daughter also accuses me of this, but having chatted to her about it, there is a secret pride there in her old dad, so I don’t mind too much). This fracture in perception, the understanding that the world is a very different place from what we understand to be internally, is what makes Gerds, Gerds. We withdraw

from the superficiality of human interaction with its movable values and eccentricities into a more clearly defined space, where the rules are more easily learned and rigorously enforced. Take computing for instance, no matter how much you yell at a computer, or how expensive your suit, or how important the deadline, or how much you love it (or lust after it for that matter) – it will not work unless you play by a strict set of immutable rules. Try applying that methodology in the workplace. People get promoted on the basis of gender, looks or connections, they are fired for speaking the truth. The power of personality rules and corporate culture then becomes an amalgam of those who most effectively play this very subtle game. In other words success regardless of talent, experience, logic or knowledge. No wonder Gerds retire to a quiet corner with a thick book or a green screen terminal and a tape drive.

Society has this pathological addiction to classifying and judging people on such superficial metrics as looks, fashion, intelligence, money, education, race, nationality or gender. Like everyone else on this planet, I am an unique individual of value. Treat me as such and do not fold, spindle or mutilate. Hence my pungent distaste at being labelled a Gerd or indeed “Deep”. Please feel free to categorise me as such, provided I can categorise you as a living testimony to a grey mush of social conformity. Unless of course you are a Geek or a Nerd, in which case I will take it as a compliment from a peer.

Ironically, my employer is sending everyone on a diversity and equality training course, and I have prepared well for this. My Unix beard is long but neat and my hair is just long enough to form a decent ponytail. Maybe I should just hand this article in instead.

---

## ROB SOMERVILLE

*Rob Somerville has been passionate about technology since his early teens. A keen advocate of open systems since the mid-eighties, he has worked in many corporate sectors including finance, automotive, airlines, government and media in a variety of roles from technical support, system administrator, developer, systems integrator and IT manager. He has moved on from CP/M and nixie tubes but keeps a soldering iron handy just in case.*

# GEEKS VERSUS NERDS

**“If you’re moving information into the cloud, it just seems to me that all kinds of nasty activity could go on in there. I would take a Missouri approach and say – prove it to me, show it to me – how it’s more secure”.**

**A**ir Force General John P. Casciano (a former director of intelligence, surveillance and reconnaissance air and space operations for the US-AF) said “If you’re moving information into the cloud, it just seems to me that all kinds of nasty activity could go on in there. I would take a Missouri approach and say – prove it to me, show it to me – how it’s more secure”. With increasing pressure on budgets and resources, more and more organisations are looking towards moving their IT operations to the cloud. Is this a genuine dawn of a new technical revolution or are we potentially facing a major crisis further down the road?

Talking to an external consultant this week I raised my concerns about the thorny question of how – from an operational perspective – there is often a major disconnect between IT and senior management. Moving on from there, the subject of the cloud came up and I was astounded by the response when I expressed my doubts about the viability of the cloud, especially where security and confidentiality was paramount. To précis, the response was basically “If the government says it is OK and secure they can carry the can if the wheel falls off”. While I admire the level of pragmatism in bolstering the latest current management thinking, this confirmed to me once again that a) Technological hype will always trump common sense and b) in the relentless pursuit of efficiency and cost savings he who ignores the adage “Penny wise pound foolish” will eventually suffer both capital and reputational loss.

Both Microsoft and IBM performed a minor miracle in the 1980’s in democratising information technology – the end user was in control (albeit to a degree and at a cost) that was impossible under centralised, mainframe big-iron. Ironically, at board level exactly the same arguments were used then as are now regarding the cloud – you don’t want your organisation held hostage by a bunch of mission critical “specialists” that

might want better pay or conditions, or heaven forbid more investment in technology or infrastructure. “Thin the herd” was the cry, and as a result the IT industry fractured and spawned a plethora of roles but all that happened in reality was a transference of control to outside the organisation and a corresponding decrease in efficiency and customer service values. It is a lot easier to walk into IT and ask a favour than logging an external help-desk call and submitting yourself to the humiliation of a rigorously enforced Service Level Agreement. Call me old school, a dinosaur – I care not. I worked in IT before the SLA and the dreaded words “Expectations management” were *de rigour*. Customer service was IT policy and we were only happy when our customers were happy. Everyone was working for the same organisation with the same goals, priorities and corporate identity. Now we have the scenario where developers, system admins, project managers *et al* are external resources and in the typical scenario the vision is that market forces will prevail by bringing more efficiency, cost effectiveness and economies of scale to the table. Alas, all this fragmentation has wrought has been increased costs, deteriorating communications, lack of creativity and ingenuity and a “one-size fits all” mentality that has turned IT from a colourful exciting career providing solutions and service to a bland bureaucratic fire-fighting exercise or worse still, being in the role of consultant where by the very insecurity of the job itself means that you are there to provide what the client wants rather than dare to rationally debate what is the best solution. I have lost count of the number of freelancers who have said to me off the record “I know it is a bad solution, I wouldn’t do it myself, but it is what they hired me to do”.

As far as any modern organisation is concerned, IT holds a very intimate and critical role in respect of how it performs. However, this is no excuse to place IT on

a pedestal. If I was CEO of a company, my first concern would not just be of one efficiency, but of adding value and growth as well. Critically though, I would understand that success is based not just on tangibles like the balance sheet, but the many subtle currents that are invisible like synergy, personal chemistry, teamwork, relationship and vision etc. These are the invisible drivers of success, and are part of the hard to quantify metric that turns an organisation from good to great. Ultimately though, it comes back to power. Success is often at the hand of the benevolent dictator. As organisations have grown larger, like the IT industry itself they have fragmented more and more with the creation of specialised roles such as HR, Accounts, Health and Safety etc. While it is undeniable that medium and large sized organisations need these departments, the unforeseen consequence of this is not just the delegation of power, but further disconnect and division within the organisation itself. So rather than promoting efficiency, the CEO is ironically held hostage to departmental silos and the organisation becomes politicised, institutionalised and inflexible. Inter-departmental rivalry becomes a matter of corporate survival, and rather than focusing on the customer, the problem becomes the lack of cohesive leadership and vision as everybody is working in isolation. The IT parody about "Herding cats" has become the corporate meme.

The cloud is meant to be a part of the solution to this conundrum, as everyone will have a single view of the organisation, their customers etc., available from every device 24/7. However, unless the culture of the organisation is mature, well developed, accepted, agreed to and understood, there will always be a window of opportunity for the unethical, exploitative and opportunist to leverage and distort an organisations' values to their own end. To quote Casciano, show me where having additional layers of management, infrastructure, legislation, personnel, policy and culture increase security. I must admit here to using creative licence. While Casciano was probably referencing security in terms of black hat hackers, spies and trouble-makers, I prefer to use the term "secure" in a much more holistic sense.

While the cloud is great for flexible processing resources and accessing non-critical data, any organisation considering implementing an IT strategy where core business is based in a public cloud without con-

siderable redundancy and professional legal advice really needs to think more rigorously. A private cloud is a much better risk, but then the cost potentially rises way above the utilitarian public offering – cheap "everything" due to economies of scale. Those old enough to remember the first generation of ISP's will remember the tension between cost of provision and virtualised web servers, and the resulting flight of mission critical applications away from virtual hosting to dedicated servers once the developers or architects realised there was an issue with scalability and performance. With the cloud, we have kicked the problem a bit further down the road, and it will be the SaaS or IaaS provider who will have to deal with the issue and inevitably will hold the better commercial hand. Already we are seeing dissatisfaction with spiralling costs and excessive downtimes due to centralised failure.

Any professional gambler will tell you of the need to spread risk. Placing all of one's eggs in a very public basket controlled by a global brand name whose sole unique selling point is trust – in my opinion constitutes a poor commercial decision. As we all know, when IT partners fall out often the only redress is often through the courts – and this is my biggest concern about the cloud. In a globalised society, who knows the legal incorporation of a local office. This might be fine for US corporations, but in Europe and elsewhere it is a minefield. Recently, a US magistrate judge ruled that Microsoft had to comply with a warrant asking for data held on their servers in Ireland. Microsoft is currently fighting this, and potentially this could end up with a major spat between US and EU courts over jurisdiction. Add to this all the additional points of failure, the ultimate loss of control, and I can see a few deeply embarrassed CEO's lining up to take the walk of shame. Have a great 2015 and for those that don't get where I am coming from, I shall finish with one word. Sony.

## ROB SOMERVILLE

*Rob Somerville has been passionate about technology since his early teens. A keen advocate of open systems since the mid-eighties, he has worked in many corporate sectors including finance, automotive, airlines, government and media in a variety of roles from technical support, system administrator, developer, systems integrator and IT manager. He has moved on from CP/M and nixie tubes but keeps a soldering iron handy just in case.*

 **Dr.WEB®**  
since 1992



# Dr.Web 9.0

## for Windows — the rapid response anti-virus

1. Reliable protection against the threats of tomorrow
2. Reliable protection against data loss
3. Secure communication, data transfer and Internet search



© Doctor Web  
2003 — 2013

[www.drweb.com](http://www.drweb.com)

**Free 30-day trial:** <https://download.drweb.com>

**New features in Dr.Web 9.0 for Windows:** <http://products.drweb.com/9>

**FREE bonus — Dr.Web Mobile Security:**  
<https://download.drweb.com/android>



# Meet the Developer-Friendly Payment Solution



## 3 easy steps to optimized checkouts:

1

### Create the checkout page

With Gate2Shop, you can optimize your payment pages by using ready-made templates or by customizing payment pages to your site look and feel.

2

### Test and optimize

An effective payment page variant testing tool, A/B Testing helps you gain insight into user behaviour, increase payment conversion in the short and long term.

3

### Accept payments worldwide

With dozens of alternative and local payment methods offered in multiple currencies, the personalized checkout allows you to reach users from all around the world.

✓ Easy integration   ✓ Cross-platform   ✓ Secure



Call for a free consultation: +44 20 3051 0330

[www.g2s.com](http://www.g2s.com)

# Take your Android development skills to the next level!

Whether you're an enterprise developer, work for a commercial software company, or are driving your own startup, if you want to build Android apps, you need to attend AnDevCon!

# AnDevCon

The Android Developer Conference

## July 29-31, 2015

### Sheraton Boston

Right after  
Google IO!

- Choose from more than 75 classes and in-depth tutorials
- Meet Google and Google Development Experts
- Network with speakers and other Android developers
- Check out more than 50 third-party vendors
- Women in Android Luncheon
- Panels and keynotes
- Receptions, ice cream, prizes and more (plus lots of coffee!)

Android is everywhere!  
But AnDevCon is where  
you should be!

Earn your Certificate!

Enhance your skills and professional qualifications as an Android expert with over 23 hours of hardcore Android training!



"There are awesome speakers that are willing to share their knowledge and advice with you."

—Kelvin De Moya, Sr. Software Developer, Intellisys

"Definitely recommend this to anyone who is interested in learning Android, even those who have worked in Android for a while can still learn a lot."

—Margaret Maynard-Reid, Android Developer, Dyne, Inc.



Register Early and Save at [www.AnDevCon.com](http://www.AnDevCon.com)

A BZ Media Event      #AnDevCon

AnDevCon™ is a trademark of BZ Media LLC. Android™ is a trademark of Google Inc. Google's Android Robot is used under terms of the Creative Commons 3.0 Attribution License.