

NOT ON LOAN

In the July 2013 issue, David Alan Grier's Errant Hashtag column, "Short-Term Loan," discussed engineers who move into management after five years. I worked for HP for 21 years and never once moved into the management track, though I toyed with the idea a few times. When I asked my boss what it was like being a manager, he said, "The first thing they do is take away your compiler." He knew me so well; he knew I would not be happy if I wasn't writing code. I never looked at management again. Being within HP in the US, I was able to stay in engineering and be successful.

However, I have observed that in the cultures of other countries, such as Mexico and India, you're a failure if you are not moving up the management chain. In presentations I have given in the US, and twice in Bangalore, I bring that up: I say that to put out a quality product, you have to have a fairly stable team of engineers that have been through several product cycles. And I tell them that the pressure and culture (outside the US) to move into management is hampering those countries' ability to produce quality products.

I'm not saying that no engineer should go into management. There are those who are born with innate management skills and those with innate engineering skills. My skills are in engineering, and I'm more than happy to let those who have the management skills manage. My ranking would have gone down had I moved into management and tried to compete against those who have natural abilities.

I wonder if there's ever been a study of what is the average age of an engineer when he or she invents a major product or receives a patent. It would be interesting to see how many occur during the first five years of their

career vs. later. I can see that college professors, like Dr. Grier, stay productive because they invent and then have (or manage) the graduate students to try it out.

Gary Stringham
gary@garystringham.com

David Alan Grier's response:

Mr. Stringham makes a good point. There are a variety of engineering careers that work on different timetables. Although we know that many engineers make the bulk of their technical contributions when they are young, it's not a given that their career must shift into management or that they must produce a uniform stream of patents every year. An engineering education can be used in many ways and can allow anyone to reinvent themselves to take advantage of new opportunities.

ISN'T THAT SPECIAL?

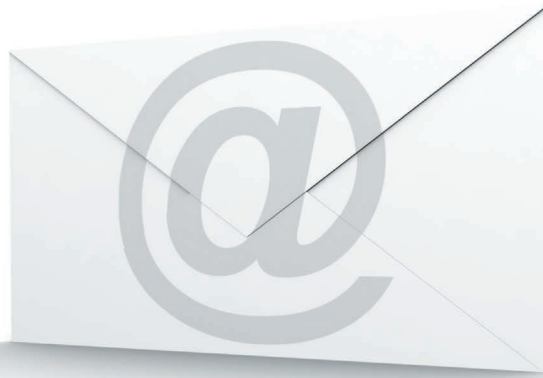
Bravo!

In the May 2013 issue, David Alan Grier's Errant Hashtag column, "The Comfort Zone," raised a recurring theme of the modern world: there are so many different *disciplines* and yet at the same time, there are very similar patterns of methods, or algorithms, among them. It makes you wonder why there are

so many special interest groups (SIGs) in every profession. Maybe what is needed is a General Interest Group (GIG) so that all the SIGs can get to know what they share in common. The perennial arguments about what software engineering is or is not, or what computer science vs. information science vs. information technology vs. data science are, are also of this pattern.

One thing is clear: the boundaries of these disciplines are diffusing into each other in ways no one imagined 20-30 years ago. In 1959, physicist C.P. Snow lamented that the boundary between the arts and sciences was wide and growing wider. Since then the boundaries separating all disciplines and specialties have blurred to such a degree that defining them is a constant source of dispute. It is time to take a 300,000 km-high view and get some perspective. The rapid pace of technology changes provides no respite to reflect on the vast landscape.

Although all of us feel some comfort in our default zones, it is time we exit them and become much more familiar with scopes that encompass the general vs. the special interest. Who



iVCE 2014

The 6th International Workshop on Internet-based Virtual Computing Environment
Oxford, UK, April 7-11, 2014

<http://www.sei.pku.edu.cn/conference/ivce2014>

in conjunction with IEEE SOSE 2014



With the fast development and wide application of computing and network technologies, the Internet has become an important information infrastructure for modern society. Today, there are unprecedented amount of resources over the Internet, e.g. content, storage, computing powers and even human presence, there is an increasing need to build large-scale parallel and distributed system over the Internet to utilize various idle resources to get better overall performance, or simply get the task done.

After years of research and practice, e.g. grid computing, service-oriented computing, peer-to-peer computing, autonomic computing and cloud computing etc., many advances have been achieved, among which there is the Internet-based Virtual Computing Environment (iVCE). The iVCE is based on the mechanisms of on-demand aggregation and autonomic collaboration. iVCE can run on the open infrastructure of the internet and provide harmonious, trustworthy, and transparent integrated services for end-users and applications. iVCE can also provide Cloud services by a dynamic combination of data centers and other multi-scale computing resources on the Internet.

The aim of the iVCE series of workshops is to provide a forum for academics as well as practitioners to share their experience, leverage each other's perspectives, and discuss emerging "hot" trends in this challenging area. The iVCE 2014 workshop is to be held in Oxford, UK, in conjunction with SOSE 2014. It solicits research papers, experience reports on various aspects of Internet-based Virtual Computing Environment.

Please visit the workshop website for more information:
<http://www.sei.pku.edu.cn/conference/ivce2014>



Important dates

Submission deadline	7th December 2013
Review notification	7th January 2014
Camera ready deadline	19th January 2014

iVCE 2014

The 6th International Workshop on Internet-based Virtual Computing Environment

knows, we may even become better professionals for it.

Francis Hsu
FH@ieee.org

David Alan Grier's response:
Well said!

PRISM GUARD

In the July 2013 issue, Hal Berghel's Out of Band column, "Through the PRISM Darkly," provides a good summary of one view of the current National Security Agency (NSA) revelations that have been in the news.

The total truth is that since the World War II era, the NSA (or its predecessors) has had the ability to listen to every telephone conversation with at least one party in the United States. And the government has listened to selected calls at will.

None of this information has ever been used for anything

except to protect US citizens from attacks on the US.

While undesirable, monitoring phone conversations is necessary to protect US citizens from people who plan to do even worse things like set off suitcase nukes in 10 US cities simultaneously. I am not such a constitutional purist that I would allow terrorists to kill me instead of recording who has talked to whom. When all the facts are known, the majority of citizens agree with that.

The total truth is that the NSA has not used any of this information to hassle citizens (or legal groups set up by citizens) who want to exercise their rights to influence the direction the US government is going, as allegedly was done recently by the Internal Revenue Service and other government agencies. Instead of destroying the NSA's ability to protect the US,

we do need to ensure that the use of the information they collect is only used for national defense and is not used unconstitutionally for political purposes as the IRS is alleged to have done.

Additionally, and much more importantly, we need to put significant controls on the actions of the IRS and its use of our personal data to avoid much worse things being done to citizens than is merely imagined that the NSA could be doing.

The NSA has less data about citizens than social media and large internet-based entities already have; and the private corporations sell it to people who send you spam email and phone you during dinner.

Phone companies and ISPs already keep data about your contacts that is available through a court order. The problem is that

when trying to catch terrorists, and stop their plots, time is often of the essence and the government needs the ability to connect the dots now, not in a few weeks.

The fact is that since the linkages are already available to the NSA, if the data were also kept in their databases it would be an irrelevant distinction.

The NSA only uses the metadata to identify potential terrorists. Until a call from a terrorist has been identified, the NSA does not intentionally listen to any US calls or read any emails. If LinkedIn can tell you that you are a second level away from a terrorist, and invite you to connect with him or her, shouldn't the NSA have that ability too?

We have government agencies that we should worry about, but the NSA is not one of them.

William Adams, PE, PhD
williamadams@ieee.org

Hal Berghel responds:

The “view” that I represented in my column has historical roots traceable to documents as far back as the Magna Carta: that democratic governments derive their powers from the consent of the governed. Wording to that effect is in our Declaration of Independence, and provides the contextual framework for ours as well as many international Bills of Rights. The operative word is “consent.” The NSA’s government surveillance programs lack oversight and transparency sufficient to pass even a minimal standard for informed consent. We have ample proof that a surveilled society is an inherently unstable society.

No one is proposing that the NSA be denied access to information that is of use in preventing harm to the US from attack. Adams presents a false dilemma. As I pointed out in my column, it begs the question whether there

might be other, more constitutionally sympathetic, effective means of accomplishing the same objective. This latter question is the real one that I encourage the reader to consider. But this question cannot be intelligently addressed in a political and informational vacuum. Absent legitimate transparency and oversight, there’s no way to determine whether the information use is legal and ethical.

Adams claims that while the NSA has the ability to spy on us, “None of this information has ever been used for anything except to protect US citizens from attacks on the US.” He does not support this assertion, and, while it is quite popular, it is increasingly open to question as previously unknown patterns of government behavior emerge from their self-generated cloak of secrecy. As I write this response, Reuters correspondents John Shiffman and Kristina Cooke just published their investigation on the NSA’s distribution of extrajudicial information to the US Drug Enforcement Agency (DEA) for purposes of criminal prosecutions that have nothing at all to do with national security (www.theguardian.com/world/2013/aug/05/secret-dea-unit-surveillance-authorities).

According to this Reuters story, for the past 20 years the NSA’s Special Operations Division (SOD) has been feeding surveillance data that might identify potentially criminal activity to federal and state agencies, including the DEA, IRS, Department of Homeland Security, FBI, and CIA. This information, by NSA policy, is not to be disclosed to prosecutors, courts, and especially defense attorneys. In fact, law enforcement agents are instructed to reconstruct probable cause after the fact from non-NSA (even fictional) sources, a process known as “parallel construction.”

There has been no judicial or congressional oversight on this activity. Law enforcement and federal agencies are actively “hiding” this information from the courts and attorneys, thereby circumventing accepted practices for pretrial discovery and the introduction of exculpatory evidence. As *Guardian* reporter Glenn Greenwald noted, this is a full frontal assault on the middle section of the Bill of Rights and undermines the very foundation of what constitutes a fair trial in our system of justice.

This NSA surveillance program is fraught with legal and ethical problems—most especially that it creates an ideal environment for abuses—especially blackmail and extortion. And that may be its eventual undoing. The very same surveillance systems that enable parallel construction in criminal cases can also be used to identify tax cheats, insider trading, embezzlement, tax havens, front running, short selling, microcap fraud—in short, criminal activity that is associated with people and corporations with enormous political influence and endless legal resources. If and when they say “enough,” the laws will change. Until then, stay tuned.

Hal Berghel
h1b@computer.org

We welcome your letters. Send them to letters@computer.org. Letters are subject to editing for style, clarity, and length.