

Privacy and Security: The *Enemy* of The Future

Keynote Speech

by

Prof. Peter A. Freeman

ENISA-FORTH Summer School on Network & Information Security

Crete, Greece

14 September 2009



Good afternoon!

Why do I assert that privacy and security is the enemy of the future?

Don't we want to have more security in the future in a world that is becoming less secure by the day?

Don't we want to preserve what privacy we still have and even restore some of what has been lost?

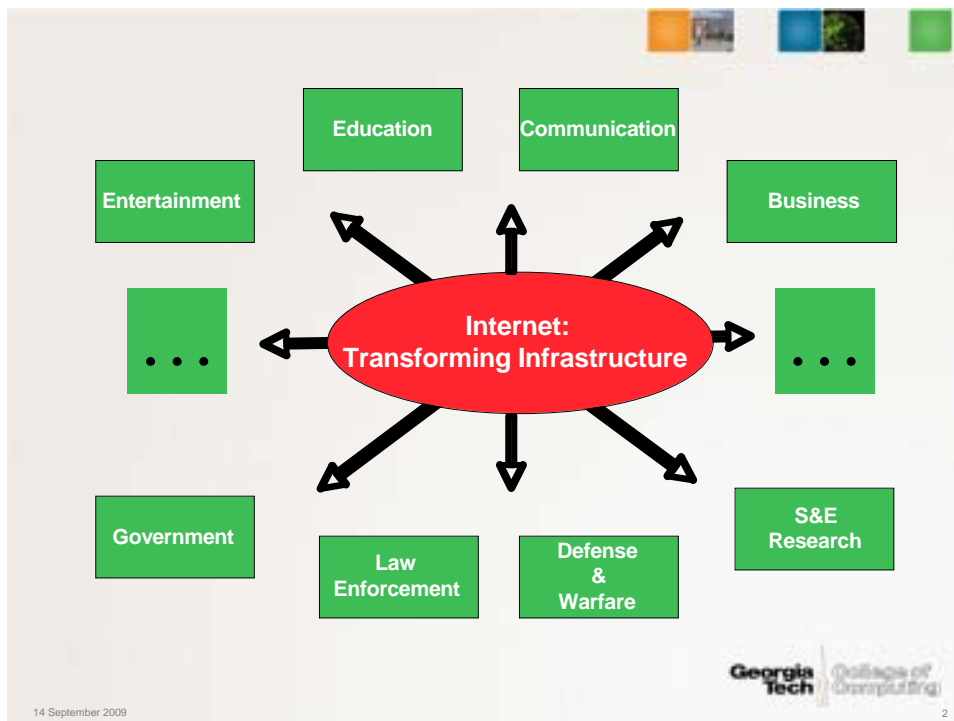
Don't we want the improvements in the future that we can already imagine?

Of course, we do!

So, my assertion must still be puzzling – especially in the context of this summer school in which you are focusing on privacy and security in a networked world – a world that is rapidly developing before our eyes.

The answer is not entirely a riddle, but let me elaborate.

I think we all agree that the Internet changes everything.




It is clear that the Internet has already fundamentally changed many of the activities in which modern societies engage and depend – commerce, manufacturing, control of the built environment such as power lines and buildings, transportation, education, research, government, defense, politics, and communication. These transformations are continuing in depth and expanding in scope, and may be accelerating. The prospects for improving health care, dealing more intelligently with the natural environment, production and use of energy, personal interactions, and general societal improvement are starting to be understood.



THE INTERNET ALSO BRINGS..

- Undesired information
- Intrusive advertising
- Erosion of cultural identity
- Intellectual property & identity theft
- Fraud
- Extremism
- Terrorism
- Potential bodily harm or even death

At the same time, the Internet has brought or increased some undesirable things – spam, erosion of cultural identity, IP theft, financial fraud, increased extremism, terrorism, even bodily harm or death. While none of these are new events – some are thousands of years old – the speed, ubiquity, and ease of access to the Internet by almost everyone in a large and increasing part of the world has given them new dimensions and severity that we must deal with.



HOW DID WE GET HERE?

- Bad things & even some benefits lead to loss of privacy
- This leads to a loss of trust in systems
- Even loss of trust in friends
- These are just symptoms
- Security (or lack thereof) is the root cause

No privacy without security!

Georgia Tech College of Computing


14 September 2009 4

These undesirable things – and, indeed, many of the positive aspects of a networked world, such as the ability of authorities to control crowds and detect crime – lead to a loss of privacy for individuals. This leads to a loss of trust in networks and in the organizations that build, own, and operate them. This lack of trust sometimes extends even to individuals that we know and otherwise trust, but whom we fear may send us infected files or inadvertently disclose our personal information.

But loss of privacy and trust are only the symptoms. Underneath all must be the technical ability to keep information private, to prevent unauthorized release of information, and to prevent unauthorized entities from changing information inappropriately. In short, there can be no privacy without security.

I assume that all of you at this summer school understand and largely agree with me, so far. So, again you must be asking, “Why is he asserting that privacy and security are the enemy of the future?”

Before I explain myself, let’s take a very brief look at what is coming down the road technically.



NEW TECHNOLOGY

- Near ubiquitous network access & usage
- Convergence, mashups, vast databases
- The Internet of Things
- Vastly increased bandwidth
- Video, advanced software, sophisticated sensors ...

We have only begun to see the problems!

Georgia Tech College of Computing

14 September 2009 5

It is reasonable to expect that within a relatively few years essentially all of the world's population will have access to the Internet either via mobile phones or some other sort of connected device. According to the ITU, at the end of 2008 there were over 4 billion cellular accounts and already almost one quarter of the world's population was using the Internet in some fashion.

The EC just reported that in Europe half of the households now have broadband, over 80% of businesses do, and there are more mobile connections than there are people – 119% penetration!

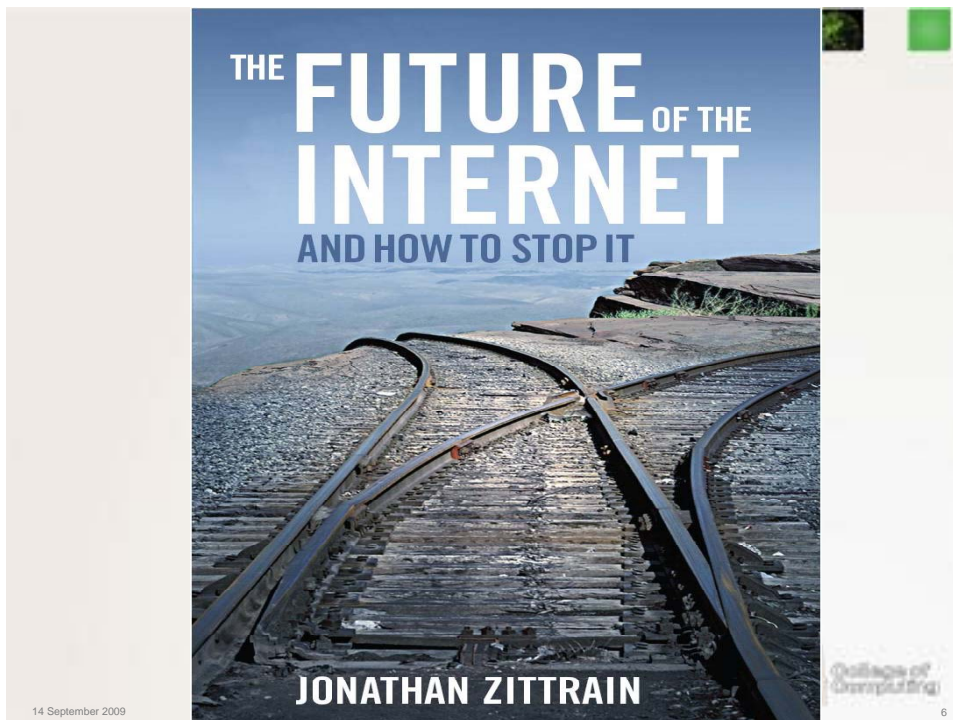
The convergence of devices and services (mashups of web applications, phones that surf the web and play music, vehicles that constantly make their precise location known to a home base) and the ability to store unheard of amounts of information online are here and growing rapidly. We've only begun to see the uses to which these devices and services can be put.

The “internet of things” in which billions – even trillions – of devices with various embedded sensors are interconnected is technically feasible and rapidly coming into being. While we think of these devices, ranging from RFID tags to light switches to refrigerators to manufacturing machines to automobiles to medical devices as primarily communicating with each other or a human operator for the purpose of improving their functionality and control, the opportunity for recording and transmitting information about us and our actions is limitless.

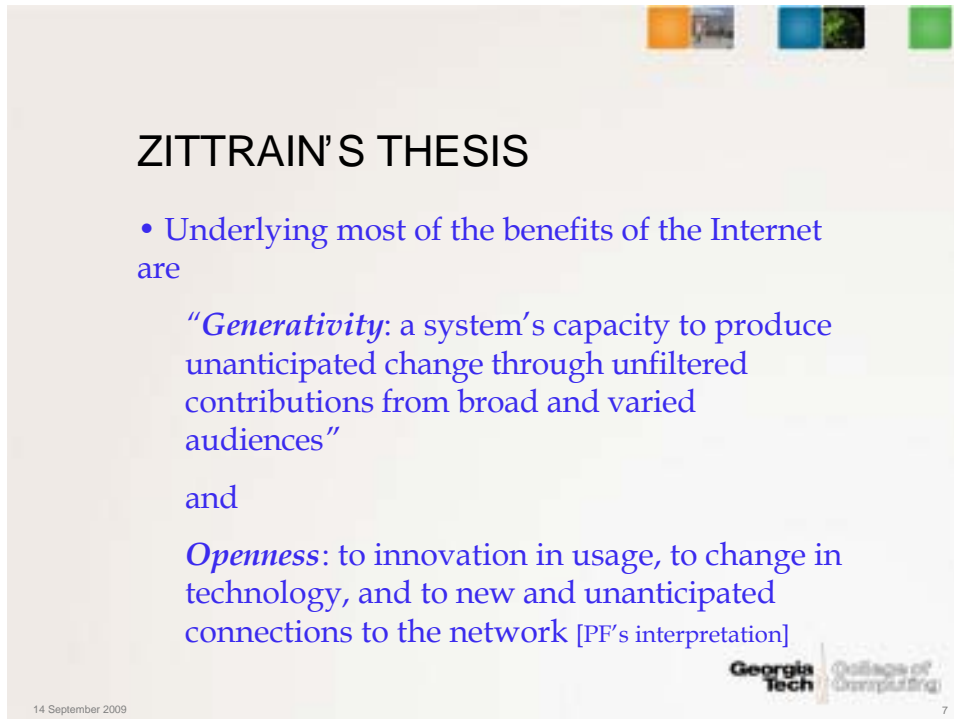
The ability to transmit large amounts of information via networks was well established some years ago. The technology of optical transmission has far exceeded what is deployed, but mass demand for video and other high-bandwidth applications is rapidly pushing wide implementation of broadband. Several years ago at NSF we funded a research project entitled “100 megabits to a 100 million homes” to investigate the issues of such wide deployment. Some technologically advanced, geographically compact countries like Japan and Korea are rapidly making research projects like this into a reality.

I could go on to describe the advances in video technology and processing, sensors of all kinds, medical devices, and so on, but this is not meant to be a technology review. My point is twofold: First, if you think today’s deployed technology is causing problems, just wait until tomorrow. Second, these projections are based on fairly obvious usage patterns and on initial demonstrations already underway in laboratories around the world. Even more radical developments may emerge from the technical domain.

Now, to explain partially my bold assertion that privacy and security is the enemy of the future, let me utilize the work of a very articulate scholar, Jonathan Zittrain of Harvard.



Here's the cover of Zittrain's recent and provocative book, in case you haven't seen it. If you look carefully, you'll notice that the track switch is set so that an approaching train (the Internet) is going to plunge over the cliff. He believes that is where we are headed and he wants to stop that projected future – not stop the Internet!



ZITTRAIN'S THESIS

- Underlying most of the benefits of the Internet are

“Generativity: a system’s capacity to produce unanticipated change through unfiltered contributions from broad and varied audiences”

and

Openness: to innovation in usage, to change in technology, and to new and unanticipated connections to the network [PF’s interpretation]


Georgia Tech College of Computing

14 September 2009 7

In his book, he outlines what he believes are at the root of the profound changes that the Internet has enabled: generativity and openness.

Generativity is a system’s capacity to produce unanticipated change through unfiltered contributions from broad and varied audiences. **Openness** refers to innovation in usage, to change in technology, and to new and unanticipated connections to the network.

These definitions are easy to understand and we all have experience with them. While they may not be the only root causes of the benefits, and undesirable things, we are seeing – widespread use is another – I would certainly agree that they are essential.



- Problems motivate users to utilize locked-down appliances (e.g. mobile phones) and services (e.g. many Web 2.0 applications) that prevent problems
- Security and privacy are gained, but generativity and openness are lost
- A security/privacy watershed will cause a rapid move to appliances and closed environments
- The result will be to go over the cliff - lose the immense, future advantages of the Internet

14 September 2009

Georgia Tech College of Computing

His argument is simple: The problems that generativity and openness permit push most people to want and adopt “locked-down appliances” like cell phones that are tethered to special purpose networks. This controls many of the undesirable effects of the open Internet while providing increased security and privacy, but at the cost of the two essential characteristics – generativity and openness - that have led to tremendous applications like Google that have come out of nowhere.

He paints a plausible scenario that sometime soon – it could be while we are talking today and it could be in several years – there will be a security/privacy watershed that convinces the public that something has to be done. This watershed might be a sudden catastrophe such as a widespread worm that suddenly shuts down the world’s financial, transportation, and communication systems, or it might be a more slowly developing situation (“death by a thousand cuts” is the phrase Zittrain uses) such as people refusing to use email because of spam until a snowballing effect takes place and no one uses email. The result will be a public and political reaction that will demand less openness and generativity. In effect, this will destroy the potential of the Internet for future innovation – run it over the cliff!



WILL THIS HAPPEN?

- Nothing is certain, but the probability is that an extreme public and political reaction will occur
- Consider some of the reactions to the illegal copying of copyrighted material
- Other, powerful interests pose various threats to an open and generative future

He may or may not be completely right in what he portrays – or in the potential remedies he outlines – but a number of us think he is largely correct in pointing up that if we don't deal with security and privacy – something that for the most part all of us have NOT done – then the consequences will be severe and will change the current Internet in dramatic ways. Some of the reactions we have already seen to problems give his argument added credence – for example, some of the laws proposed and even passed in the US to combat IP piracy.

Whether or not changes that destroy generativity and openness are desirable is an on-going and fierce debate. There are other proposed changes that would radically alter the Internet, ostensibly for other reasons, but that may stem from privacy and security concerns. They often involve huge corporate interests such as the Recording Industry Association of America (RIAA) that aggressively pursues copyright violators, and some of the common carriers that would like to have more control over what they transmit (the “net-neutrality” argument). It involves legal scholars such as Larry Lessig who believes that changes to copyright laws that have been driven by corporate interests in protecting their intellectual policy are destroying our intellectual commons that has led to much of our current culture. Researchers and technologists worry that their ability to innovate will be restricted, while law enforcement authorities want to extend their

control, and some nations seek to restrict what their citizens can see and do on the Internet.

Some argue that fixes can be added to the Internet. Others argue that there is no reason that both tethered appliances and the open Internet can't co-exist. They may be partially right, but at the moment there is great potential for harm.

Let me hasten to point out that Zittrain is not saying that privacy and security is the enemy of the entire future – only the future of the Internet. I'm responsible for asserting the extension.

WILL THIS STOP *EVERYTHING*

- Zittrain does not assert that
- I exaggerate to make a point
- Any innovation is based on information, communication, and exploratory tools
- The Internet provides these as nothing else does
- If we restrict the Internet unduly then we are restricting these foundations of innovation
- We will be restricting the future

Georgia Tech College of Computing

14 September 2009 10

My almost 50-year involvement in computer research and development leads me to the conclusion that at the core of innovation in all fields is information, communication, and tools that help the innovator explore new ideas and things. That is what the Internet does to an extent that nothing before has done and that is now threatened by over-reaction to security problems. That is why I assert that it is not just the future of the Internet, but the future that is threatened.

So, what can and should we do?

There are a number of things that we can each do individually and in our organizational roles, but let me describe briefly the response that I led at the US National Science Foundation (NSF) while I was there and with which I'm still involved.

As context, let me explain that NSF, as a part of the US Government, has the responsibility to support – not perform – basic research in all fields of science and engineering. The work is largely done at universities that are dedicated to generating new knowledge and educating tomorrow’s researchers, innovators, and leaders in all fields. To understand what research needs to be done, NSF regularly convenes groups of scientific, business, and other leaders to develop cohesive understandings of what is most needed.

ORIGINS OF THE GENI PROJECT

- Growing concern was expressed in the technical community about future network capabilities
- At the same time, rapid expansion of critical use of the Internet for many purposes by many users was taking place
- Extent and severity of problems were growing exponentially (still are!)
- NSF took the lead in addressing the situation

Georgia Tech College of Computing
14 September 2009 11

NSF has a long history, dating back to the late 70’s, in helping create and implement the current Internet, so it was natural that starting in the late 90’s they convened a series of workshops to address the question of what networking research was needed to prepare for the future. One of the first was conducted by an organization headed by one of the recognized “inventors of the Internet,” Bob Kahn. The last of that series of workshops was held in early 2002 just as many of the current security and privacy problems of the Internet began to make a strong impact on the public.

Indeed, there were several political/legal reactions at about the same time in the US that led to some good actions such as legislation authorizing (but not entirely paying for!) greatly increased research on computer security and some that were later struck down because of their overreaction to the problems. Many of those types of legislative and governmental actions – both helpful and less so – continue worldwide.

By 2002, we knew at NSF that some fundamental changes were needed in networking research to prepare for the future and started taking actions to address those research needs. In 2004, a set of ideas developed in conjunction with some senior leaders in the networking community that resulted in the GENI Project.

NSF's RESPONSE IN 2004-2005 WAS:

- Emphasize experimentation and theoretical development
- The GENI Research Program, focused on experimental/theoretical foundations for future network design
- The GENI Facility, to provide an instrument for at-scale experimentation

Georgia Tech College of Computing

14 September 2009 12

Clearly, one of the primary drivers for undertaking this major project was the rapidly increasing and serious issue with computer security. As a result, our primary objective was precisely the same as the subject of this week's summer school – privacy and trust.



THE FUTURE GLOBAL NETWORK

Should

- Be worthy of society's trust
- Provide a bridge between physical and virtual worlds
- Support pervasive computing
- Enable further innovations in research and commerce
- Create a world in which we would want to live

At the same time we recognized that there are other important objectives including innovation and being able to deal with the coming explosion of devices on the Internet.

We parsed the challenges we faced into five categories.



CHALLENGES

- Technical (e.g. security)
- Social (e.g. children's use)
- Political (e.g. posting false info)
- Policy (e.g. access)
- Legal (e.g. copyright)

These fundamental issues are closely intertwined and must be addressed if we are to realize the opportunities before us.

We could not simultaneously address all of them, so the project was largely technological at first, focused on providing an advanced networking environment that would support serious and realistic experimentation with everything from new optical techniques to new pricing techniques and not-yet-invented applications. I believed then and still do that fundamental changes in the architecture of the Internet will be necessary, all the while keeping in mind the necessity of not destroying the value of generativity and openness that have been so influential.

The design of the GENI Facility – the instrument by which researchers can experimentally explore new architectures and policies under realistic conditions continues and is now at the prototyping stage. The research program has evolved into a comprehensive program (NetSE – Network Science & Engineering) touching on many aspects and like any research program will take time to produce new results. I provide some references to the research agenda and other material on GENI at the end of this talk.

Let me take a moment to outline the research scene on privacy and security in the US since that is your focus this week. It is widespread today and in some instances dates back many years. It ranges from development of new encryption techniques to social studies of the impact of lack of privacy on individuals to studies of copyright law in a networked world to economic studies. NSF has supported research on privacy and security that addresses basic issues applying in many situations, as well as research more specifically focused on networked environments.

The teams that are prototyping the GENI facility include work on basic technical security mechanisms. The broader NetSE Research Agenda came out of a series of workshops, one of which was focused on network design and societal values – more generally, the interplay between technical design and political/social life.

My purpose today is not to describe the details of this continuing project, which is now mirrored by projects in Europe, Japan, and elsewhere, but to emphasize a point: Namely, that dealing with privacy and trust in a networked world must begin with having the technical means of providing security. Further, in something as complex as the Internet with its multiple levels and broad reach, it is essential that one have a foundation of experimentally verifiable knowledge on which to base design and policy decisions that are as solid as possible. One would not set out to design a new aircraft without a huge amount of scientific and experimental knowledge, or to establish policies for the operation of hospitals without

extensive empirical information and medical knowledge. Designing a Future Internet and the policies around it should be no different.

Let me conclude with some policy and decision issues and guidelines.

One of the acknowledged leaders in the networking technical and policy security world, Professor Gene Spafford, recently listed for me his top observations about our current responses to privacy and security issues:

The slide is titled "SPAFFORDS OBSERVATIONS" and lists five key observations in blue text. At the top right, there are four small colored squares (orange, blue, green, and a darker blue). At the bottom right, the Georgia Tech logo and "College of Computing" are visible. At the bottom left, the date "14 September 2009" is shown, and at the bottom right, the number "15" is present.

- Politicians require a crisis before acting
- Authority and responsibility are usually separated
- We lose privacy a tiny bit at a time, to our surprise
- Global problems are also local
- Getting the job done usually trumps security

- There has to be a crisis for politicians to act – for example, to put proper security policies in place, pay for the needed equipment and operational activities to make such policies effective, or to pay for research to prevent future crises.

- Leaders of government or industry often won't connect authority and responsibility. For example, most CISO's (Chief Information and Security Officers) are responsible for security, but usually don't have the authority to make people do things differently or even to buy equipment and services to help make them secure.

- Most people are willing to give up little bits of their privacy (e.g. identifying themselves when making a purchase in a store) for some small reward or convenience, and then are surprised and even outraged when they

discover that they have cumulatively lost a lot of privacy, or worse, are seriously damaged.

- Problems are not only global in their reach no matter where they originate, they can be expected eventually to impact people and organizations even in the originator's country or region.
- Issues of usability, efficiency, and mission of the organization usually trump security (e.g. security policies and mechanisms will be ignored or circumvented if necessary, with little or no penalty).

Some of these points may be somewhat US-centric, but I'd be very surprised if there are not European analogs. While they are stated in the form of observations, the policy and decision guidelines they suggest should be obvious.

He went on to list his top concerns about operational privacy/security:

The slide is titled "SPAFFORDS OPERATIONAL CONCERNS" and lists five concerns in blue text:

- Lack of metrics
- Lack of balance between privacy and security
- Obscured side-effects
- Unforeseen consequences
- Overdependence on technical measures

The slide also features the Georgia Tech logo and the text "College of Computing" in the bottom right corner, and the date "14 September 2009" in the bottom left corner.

- Lack of security/privacy metrics: How can we measure progress if we have no metrics?
- Lack of balance between privacy and security: Efforts to provide security too often erode privacy by requiring too much information about you for authentication.
- Obscured side effects: Lower cost or other enticing features lead to adoption of technologies that may ultimately reduce privacy and

security. Example: Cloud computing. You no longer control your own data and thus can't be certain of who sees it!

- Unforeseen consequences: Example: Convergence of devices. When everything is linked and compatible with everything else, we may see the emergence of scams in which compromised computers call your friends and speak with your voice to try to get private information.
- Overdependence on technical measures: Although laws and social attitudes change slowly we must have stronger legal and social responses against misfeasors, not just higher technical walls.

Jonathan Zittrain's book provides some clear food for thought for anyone involved in making policy and making decisions. There's not time today to provide a thorough survey of policy – nor is it my role here – but I've provided a set of references for your information.

Finally, let me list without much comment or attribution of source a set of guideline questions that as a former executive and participant in setting policy that I believe are fundamental.

For a security policy or decision under consideration or being implemented:

The slide features a title 'SOME QUESTIONS TO ASK ABOUT A POLICY' in bold black text. Below the title is a bulleted list of six questions in blue text. The slide also includes the Georgia Tech logo and the text 'College of Computing' in the bottom right corner, and the date '14 September 2009' in the bottom left corner.

SOME QUESTIONS TO ASK ABOUT A POLICY

- Does it balance security and openness & generativity?
- Is it proportional to the benefit?
- Are broader interests served?
- Does it infringe basic rights?
- Will it be applicable in other countries & cultures?
- Is it based on evidence?

Georgia Tech College of Computing
14 September 2009 17

- Does it strike an acceptable balance between security/privacy and preserving openness and generativity?

- Is it in proportion to the security/privacy benefit to be gained?
- Will the broader interests of society (or, at least, the organization) benefit or is it only going to benefit a particular segment?
- Does it infringe basic rights guaranteed by law?
- Will it apply in different nations or cultures, if appropriate?
- Is it based on data and factual evidence, and have its potential consequences been carefully studied?

Experienced policy makers will likely see these as rather rudimentary – indeed, they are! Yet, they are often ignored.

Operational managers will question whether such considerations need to come into play when their task is to make decisions in a constrained environment when they probably have little or no ability to change the constraints. At one level, of course, the answer is they may be superfluous.

Yet, we all have a responsibility to help deal with security and privacy. Personal and professional integrity demands that at a minimum we raise such questions up to a level where they can be dealt with.

Devising good policies and making effective operational decisions are always going to be difficult in their details and very context-dependent. At the same time, the overarching message is: Don't diminish the great benefits of a networked world, but instead do everything possible to enhance the fundamental features that produce benefits while preserving policy and providing security.



With that expectation and bit of advice, let me wish you a good week learning more about privacy and trust in a networked world during this week's school, and even more, in applying what you learn when you return home.

The future is up to you!

Thank you.

CONTACT:

Peter A. Freeman
Emeritus Dean and Professor
Washington, DC, USA
peter.freeman@mindspring.com
www.cc.gatech.edu/staff/f/freeman/

FOR MORE INFORMATION

NOTE: This is purely an adhoc list of references to get you started. Coupled with a few Google searches, they will quickly get you into current thinking, discussion, and work on privacy and security in the United States as covered in this talk.

The Future of the Internet--And How to Stop It (Paperback) by **Jonathan Zittrain**, Yale University Press, 2008.

Zittrain's organization: <http://futureoftheinternet.org/>

Free Culture: How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity, by **Lawrence Lessig**. The Penguin Press, 2004.

Lessig's organization: <http://www.lessig.org/>

An academic group, led by **Prof. Annie Anton**, focused on privacy:
<http://theprivacyplace.org/>

Michael Nelson of Georgetown University is a frequent policy commentator:

<http://explore.georgetown.edu/people/mrn24/?action=viewgeneral&PageTemplateID=137>

Prof. Gene Spafford: <http://blog.spaf.us/>

Spafford's blog: <http://spaf.cerias.purdue.edu/>

His research center: <http://www.cerias.purdue.edu/>

Prof. Ed Felten is an active researcher and policy analyst:
<http://www.cs.princeton.edu/~felten/>

His research center: <http://citp.princeton.edu/>

Primary website of the **GENI Project**: <http://www.geni.net/>

The **NetSE program** of NSF

http://www.nsf.gov/cise/news/2008_08_netse.jsp

http://www.geni.net/?page_id=28

The division of NSF supporting a lot of networking and security research:

<http://www.nsf.gov/cise/cns/about.jsp>

Their networking program:

http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503307&org=CN

Their security program:

http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=5158&org=CNS