The New Age of Near-zero Privacy

Privacy has been greatly diminished over the past 20 or so years. Electronic data privacy, in particular, has been affected by frequent large-scale breaches of vast repositories of personal information and other sensitive data. Physical privacy has also been significantly reduced by the ubiquitous and universal deployment of digital cameras in phones, drones, facility surveillance cameras and so on. The willingness of many to share personal data and images, unaware of or unconcerned about high-risk consequences, has contributed to the privacy deficit.

This article examines this rapid loss of privacy and describes current approaches to mitigating risk of exposure of personal data and images. According to a recent Pew Research Report,[1] researchers, government representatives and industry experts are split between those who have little confidence of improvement over the next decade and those who think that some semblance of privacy might be regained. This article suggests how societies, governments and technologists might collaborate to achieve "generally acceptable" privacy.

Background

It has been approximately 17 years since Scott McNealy, founder and former chief executive officer (CEO) of Sun Microsystems, said, "You have zero privacy anyway. Get over it," before reporters and analysts.[2] Since then, there has been exponential growth in the use of the Internet and the size of data repositories, as well as rapidly declining costs for storage and processing as new technologies provide orders-of-magnitude improvements in cost and performance, such as for storage class memories (SCM).[3] As a result, exposure to data breaches, identity theft, fraud, blackmail and other nefarious practices has been growing exponentially and is expected by some to continue increasing well into the future.[4]

The Internet, social media, public record web sites, advanced encryption, anonymous transactions and the Dark Web (which provides anonymity to users and web sites and is not indexed by search engines, such as Google) have eliminated data privacy on the one hand and facilitated unfettered crime on the other. Global positioning systems (GPS), closed-circuit television (CCTV), smart phones, drones, body cameras, automobile dashboard cameras, and other means of continuously recording individuals and their activities and locations have demolished physical privacy.

> **"Are expectations for privacy, clean data and protection against 'the bad guys' unrealistic?"**

Ubiquitous surveillance and breaches of huge, highly sensitive databases have contributed to having little or no privacy—neither electronic nor physical—and lead to identity theft, fraud, blackmail, intellectual property (IP) theft, espionage and other cybercrimes. Furthermore, many data errors can be unintentionally or knowingly hidden within such vast data stores, causing wrong and possibly dangerous decisions to be made.[5]

What must be done to protect against such nefarious actions while still having the freedom to go about daily business? How might the demand for

C. Warren Axelrod, Ph.D., CISM, CISSP
Is a senior consultant with Delta Risk LLC, specializing in cybersecurity, risk management and business resiliency. Previously, he was the business information security officer and chief privacy officer for US Trust. He was a founding member of the Financial Services Information Sharing and Analysis Center and represented financial services cybersecurity interests in the US National Information Center during the Y2K date rollover. He testified before the US Congress in 2001 on cybersecurity. His most recent book is *Engineering Safe and Secure Software Systems*. Previously, he published *Outsourcing Information Security* and was coordinating editor of *Enterprise Information Security and Privacy.*

privacy be balanced against the need for national security? Are expectations for privacy, clean data and protection against "the bad guys" unrealistic? If so, what is an acceptable level of privacy compromise? If not, what must be done to resolve so many issues?

To answer these questions, one must examine the state of privacy today, how it will likely change over time, and what must be done to retain freedoms while protecting individuals and assets from human error, mischief and dangerous criminal activities. While the expectation cannot be to achieve permanent and lasting protection because both attackers and defenders are adding to their capabilities, the risk of privacy violations can be mitigated while still maintaining a secure homeland. Taking required actions calls for money, effort, courage and resolve, but this surely can be done if the will exists.

Addressing Privacy

If the consequences of technology are indeed inescapable, how can an environment be created that might be acceptable, at least to the majority?

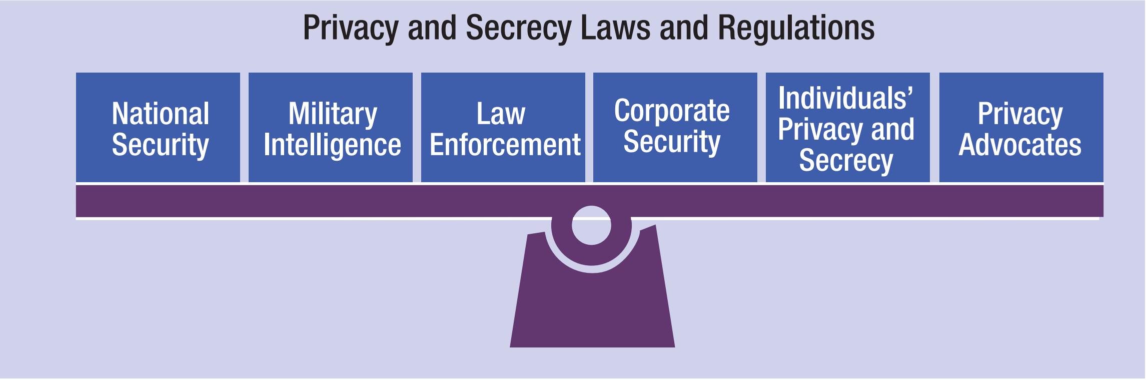
One approach is to launch a high-stakes, single-focus project for cybersecurity—a project that will "boil the ocean," as it were. The challenge of securing cyberspace is not entirely specific and is somewhat difficult to explain and justify. Furthermore, it is extremely challenging, in part, because there are diverse interest groups within every society.[6] While some regimes have been able to control specific segments of the Internet, no single country can control the entire network—although some might be able to inflict considerable harm.

Barring a gargantuan effort, the global funding and support of which is an open question can so many diverse players be influenced and persuaded to operate in the interests of the majority? David Chaum, who invented early anonomyzing networks[7] and a cryptocurrency (ecash),[8] believes that he has a technical solution. Chaum is quoted as saying: "You have to perfect the traceability of the evil people and the intraceability of the honest people... That's how you break the apparent tradeoff, this standoff called the encryption wars."[9]

A fallacy of this argument is that it depends on who is considered to be good and who is believed to be evil, who should be free to pursue certain activities and who should not, and which activities are beneficial and which are destructive. All of these issues are highly subjective. Choosing one side or the other depends on one's identity, location, background, beliefs and prejudices. Getting everyone on the same side is realistically impossible, so some compromise has to be reached.

It is in such an environment, in which both sides are vociferous and articulate, that attempts must be made to discern what to achieve in protecting

Figure 1—Balance of Privacy Across Constituencies



Source: C. W. Axelrod. Reprinted with permission.

privacy and what it is worth to do so. The context must be considered to determine how much and where society is willing to invest to facilitate needed changes. Given this backdrop, perhaps the most reasonable approach is to attempt to arrive at a point on the privacy spectrum that maximizes the total of all (good) benefits. **Figure 1** shows the balance that needs to be achieved across all positive constituencies. The "bad guys" are excluded since what benefits them detracts from the overall good rather than enhancing it.

The goal is to select a point along this spectrum that yields an optimum privacy value. Ideally, this would mean that moving away from such a point means that someone is worse off and the aggregate benefit is reduced. This point is called the Pareto optimum in the field of economics.[10] To develop this concept further, it is essential to review the history of privacy and how privacy might evolve over time.

Past Privacy Environment

There seems to be a great deal of confusion as to what privacy actually is; the differences between data privacy and the right to privacy; how privacy is distinct from security, secrecy and safety; and which data should be classified as private or secret and which should not. It is useful to view privacy as a legal right and security technology as a means to achieve it.[11]

First, one must distinguish among physical data privacy, electronic data privacy, physical privacy, secrecy, security and safety.

Privacy vs. Secrecy

In many respects, privacy and secrecy are very similar. The main difference is well expressed by Eric Hughes, as follows: "A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anyone to know."[12]

Another difference is that private data must be attributable, whereas secrets may be anonymous.[13] Further, secrets do not have to relate to persons; they can be about intellectual property, such as recipes or machine designs.

> **"The risk of privacy violations can be mitigated while still maintaining a secure homeland."**

The same means of protection, authentication and authorization, such as encryption, are often common to privacy and secrecy. However, sometimes secrets might be accidentally disclosed along with privacy-related data, as was the case with Edward Snowden's leaks, and might lead to dangerous information being made available to enemies as well as intended recipients. For both privacy and secrecy, those for whom the information is meant have to be carefully vetted.

Privacy vs. Security

The terms "privacy" and "security," as they relate to personal information, are often used interchangeably. Many experts prefer to think of privacy as a legal right with security providing the means (tools, methods, policies and procedures) to ensure that the personal information is protected against unauthorized access and use.[14]

Security vs. Safety

One set of definitions for security and safety, as they relate to software, is:[15]

- **Safety-critical software**—The software must not harm the world.
- **Security-critical software**—The world must not harm the software.

Essentially, security and safety engender different cultures, with the cybersecurity professional

Figure 2—Relationships of Privacy, Secrecy, Security and Safety Features to Privacy Rights

Examples of Privacy Rights	Physical Data Privacy	Electronic Data Privacy	Physical Privacy	Secrecy	Security	Safety
The right to be left alone	X	X	X	X		X
A desire for independence of personal activity	X	X	X	X		
The right to make decisions regarding one's private matters	X	X	X			
Space for intellectual development, anonymity or obscurity	X	X	X	X		
Freedom from public attention	X	X	X	X	X	X
Freedom from being observed or disturbed by others	X	X	X		X	
Freedom from intrusion into one's solitude	X	X	X		X	
Avoiding public disclosure of private facts about oneself	X	X				
Freedom from publicity that places one in a false light	X	X		X		X
Freedom from appropriation of one's name or likeness	X	X	X		X	X
Control of how one's personal information is collected and used	X	X			X	
Freedom from surveillance	X	X	X	X	X	

Source: C. W. Axelrod. Reprinted with permission.

focused on protecting systems and data from unauthorized access and use, and safety engineers concerned about what harm the system might inflict on persons or the environment were it to malfunction or fail.[16]

Secrecy vs. Safety

Increasingly, it is becoming possible for privacy and secrecy to affect a person's well-being. It is clear that breaches of web sites such as Ashley Madison not only damage relationships, but can lead to suicide, as was reported.[17]

Figure 2 shows examples of privacy rights[18] and indicates their coverage by privacy, secrecy, security and safety.

Until the general use of computers more than half a century ago, information was typically available in cleartext[19] on physical media (e.g., paper, magnetic tape), so that, for protection, one had to lock away sensitive information. In some cases, information was encrypted or otherwise encoded, requiring a key or rule to obtain cleartext from cyphertext. While such information could be stolen and used for nefarious purposes, it would take considerable planning and effort to do so with the result that attempts to get hold of substantial amounts of such information were generally restricted to high-value data (such as details of a pending corporate merger or military battle plans).

Physical privacy methods often took forms much the same as those used today. There are simple, cheap, passive measures such as posting signs that say "private property," "no trespassing," and "no entry." There are more assertive, though still passive, methods such as walls, padlocks and barbed-wire fences. And then there are more active methods such as alarms, guards, dogs and electric fences. These methods can also be considered to be security and safety measures to the extent that they protect persons from harm, as opposed to protecting sensitive personal and business confidential information.

Privacy Today

It is a very different privacy world today, particularly with respect to electronic data processing. Physical privacy has been significantly affected by security and safety innovations, particularly with electronic locks based on codes, fobs and biometric technology, and from connecting security systems to the Internet of Things (IoT).

Almost every day, there is news of data breaches affecting nonpublic personal information, with the perpetrators becoming more sophisticated and better funded. The marketplace for individuals' private data and organizations' secret information is huge. At the same time, the collection and correlation of these data keep growing relentlessly, and the ability to analyze the resulting big data in real time is improving rapidly and proliferating widely. Unfortunately, attempts to control the collection, use, storage and disposal of such information with tools such as identity and access management, intrusion detection and prevention systems, and the like, have appeared to do little to slow the acceleration of data breaches and compromises.

The Future Of Privacy

One of the most helpful documents on the evolution of privacy and its future direction is the aforementioned Pew Research Report.[20] The researchers obtained survey responses from 2,511 "experts and Internet builders" to the abbreviated questions in the following areas:

- **Security, liberty, privacy online**—Will a secure, popularly accepted and trusted privacy-rights infrastructure be created by 2025?
- **Acceptable balance**—Will policy makers and corporations strike the right balance among personal privacy, secure data, and compelling content and apps?
- **Privacy norms**—How will privacy in a broader social context differ in 2025 from 2015?

The respondents were split, with slightly more than half (55 percent) believing that an accepted privacy-rights regime and infrastructure will not be in place by 2025. There could well have been a vested interest in not establishing such a regime and infrastructure by this group of interviewees, whose livelihoods are based on personal data that are currently freely available. The results might have been very different if there had been larger representation by lawmakers and regulators.

The two constituencies gave predictions regarding their expectations as to whether a widely accepted privacy infrastructure would be put in place over the next decade. The respondents came up with the following themes:

- Acceptance of greater public presence and exposure
- Unprecedented ubiquitous surveillance
- Trading of personal information for convenience
- Asymmetrical arms race between attackers and defenders
- Negative effect of diverse global views on civil liberties
- Impact of new technologies (e.g., IoT)
- Difficulty in managing more complex privacy and security
- Greater power to individuals in negotiating with companies and governments
- Potential backlash from privacy breaches

Since there is a fairly even divide between those who were optimistic that a new world in which a generally accepted, trusted privacy-rights infrastructure will be established over the next decade and those who did not so believe, actionable plans that will move society toward an improved privacy environment need to be developed.

The Complex Privacy Environment

A major reason for the diversity of views as to whether or not attempts to establish a commonly agreed-upon privacy posture and corresponding infrastructure will be successful is that there are many players with differing views on the value of privacy and the need to establish greater controls.

It is important to note that the European Union (EU) has been a global leader in establishing privacy criteria for the past 20 years and has recently clamped down on the enforcement of compliance requirements. Were the EU standards to be enforced worldwide, there would be much clearer guidance on standards and their enforcement. However, the costs to those countries that are currently deficient in their compliance with the EU standards could be extremely high, both in terms of additional costs and lost business. This would engender significant resistance, particularly from those economies, such as the US, that are benefitting considerably from a lack of stringent privacy requirements.

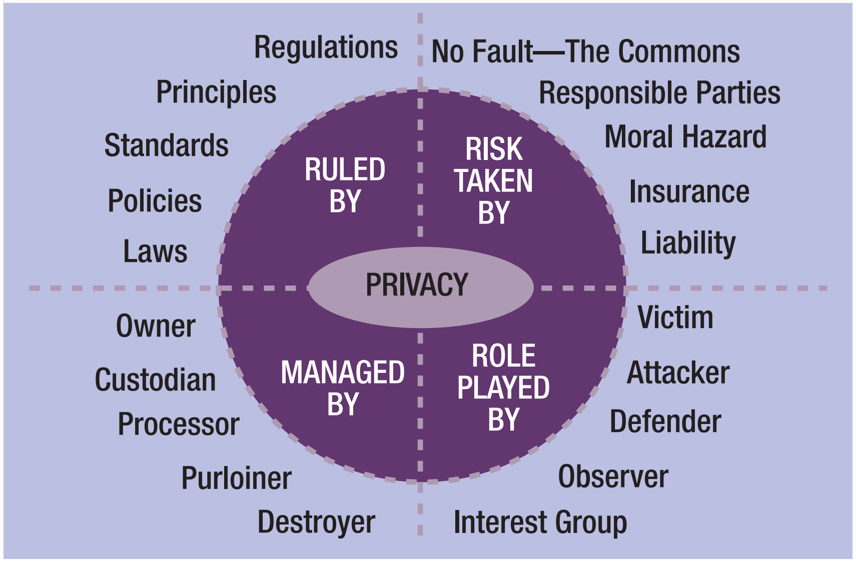
Figure 3 illustrates the complexity of trying to come to a universal agreement on privacy by showing the various constituencies affecting and affected by privacy rights and the mechanisms whereby those rights might be managed.

Rules and Enforcement

The laws and regulations regarding privacy vary significantly by country, region and culture. The EU has the most stringent rules. Some renegade countries barely pay lip service to privacy.

However, privacy laws and regulations are often not sufficiently comprehensive and do not reflect much in the way of understanding the dynamic impact of technology on privacy, secrecy, security and safety. This can be attributed, at least in part, to the disappointing lack of generally accepted information security principles and standards.

Figure 3—Actors Affecting Privacy



Source: C. W. Axelrod. Reprinted with permission.

On the other hand, there are official, Generally Accepted Privacy Principles (GAPP) the American Institute of Certified Public Accountant (AICPA) and Canadian Institute of Chartered Accountants (CICA) that include the following 10 principles:[21]

1. Management
2. Notice
3. Choice and consent
4. Collection
5. Use, retention and disposal
6. Access to third parties
7. Disclosure to third parties
8. Security for privacy
9. Quality
10. Monitoring and enforcement

However, the determination as to whether to audit and enforce privacy based on GAPP is at the discretion of auditors and not enforced by laws or regulations. One cannot expect to see much improvement in the privacy infrastructure without stringent enforcement and painful consequences for noncompliance.

Responsibilities

A significant detriment to establishing and enforcing privacy principles and standards is the lack of liability and the ease of avoiding personal consequences in many cases of privacy breach. At one time, the common lore was that a data breach would affect stock price, but this does not appear to be a significant factor over the longer term. Yes, the careers of the few who are blamed might be stymied for a while, but generally, organizations absorb the losses and expenses, strengthen their security, and proceed with business as usual. The rapid growth of the purchase of cyberinsurance suggests that cyber is just another business risk.

When a single entity is affected by privacy leaks, some measures are taken by the organization to quell the concerns of victims and reduce the probability of subsequent attacks. But when the weaknesses and attacks are systemic, individual companies and public agencies are not generally faulted and little is done to change the environment.

Roles

There are a number of different roles when it comes to data privacy protection and failure to fully protect. There are the victims, of course. They are commonly individuals who are customers of financial institutions, retail companies and the like. In some cases, as with credit cards in the US, customers are protected for proven fraud of more than US $50, for which fees are often waived. Individuals are also usually offered free credit reporting services for some period of time.

Then there are the attackers and the defenders. Attackers vary from lone hackers to organized crime to terrorists and nation states. Defenders are typically the various institutions and agencies that have fiduciary responsibility to protect personal data in their custody. These organizations may have internal security and privacy staff or may defer to third parties. And, there are observers and interest groups, including such organizations as the Electronic Privacy Information Center (EPIC), which may be purely informational or take action when privacy compromises are seen or when laws and regulations are supported or condemned.

> **“When the weaknesses and attacks are systemic, individual companies and public agencies are not generally faulted and little is done to change the environment.”**

Management

This category includes organizations that have fiduciary responsibility to individuals to protect their personal data. They also happen to be sources for insider threats. External attackers also manage privacy, but in an adverse way for their own advantage.

Dealing With the New Privacy

A number of leading professionals in the cybersecurity field have questioned the ability of current approaches to protect systems and data against cyberattacks. Amit Yoran, president of RSA, stated in an interview that: “The [cyber] security industry is failing.... It has failed.” Yoran proposes the following guidance:[22]

- **Know your environment**—Gain visibility into end points and cloud-based environments
- **Know your users**—Recognize the need for better authentication

- **Know your adversaries**—Understand external threats using threat intelligence
- **Know your priorities**—Understand business risk and value of mission-critical systems
- **Know your weaknesses**—Understand dynamic malware and resulting vulnerabilities

These guidelines provide a good basis for generally improving cybersecurity, which, in turn, leads to better protection for private information. However, this is only part of the solution, and other tools and methods should be brought to bear.

1. Build In Privacy

Just as there are very active groups supporting building security into all phases of the software development life cycle (SDLC), so, too, are there some, though relatively few, exhortations to build in privacy, meaning that privacy requirements need to be inserted into the life cycle during the initial phases and carried through deployment, use and disposal. One such advocate is Ann Cavoukian, Ph.D., the information and privacy commissioner of Ontario, Canada, who wrote the foreword for the book *Privacy: What Developers and IT Professionals Should Know*, which is one of the few books that helps designers and developers build in privacy functionality from the start.[23] To reduce vulnerability found in "the privacy functionality of a technology...used to collect and manage personal information," Cavoukian says there is "the need for privacy to be designed into an information management system, right from the beginning." If privacy functionality is not built in from the start, it is unlikely that it will be added later due to the much greater effort and cost of doing so.

2. Laws and Regulations

EU privacy laws and directives are among the most stringent in the world and have been shown to be enforceable. If significant improvement worldwide is to be seen, the EU standards should be applied universally and enforced by an entity with global reach. The importance of international cooperation in this area cannot be overstated since it is only if global authority is supported and maintained that such overarching rules can be applied.

3. Generally Accepted Privacy Principles

While GAPP has been developed and is used in North America as an auditing tool, there needs to be universal support for these principles and a means of enforcing them. Again, as with laws and regulations, such principles and standards are effective only if everyone adheres to them.

> **“If privacy functionality is not built in from the start, it is unlikely that it will be added later due to the much greater effort and cost of doing so.”**

If universal privacy laws and principles are not established and enforced, there can be little hope for ensuring privacy worldwide since if even one link in the chain is not compliant, then it cannot be certified that the privacy hurdle has been scaled.

Conclusion

There are many diverse views on universal electronic data privacy and how it might be achieved. While the technology to enforce privacy already exists or may be readily developed, it will not work unless the legal, political and social acceptance and the will to gain control of the current runaway situation are there.

Some may say that the challenge of universal privacy will not be taken on until something really bad happens. However, others might maintain that such catastrophic events have already taken place with the egregious breaches of the US Office of Personnel Management (OPM), Target stores and the like, but little to remedy the situation has emanated from these.

Given the generally observed apathy of many of those whose information has been compromised, (which might result from the enormity of the problem and the lack of confidence that it can be eliminated), there seems to be little hope of a major effort to raise data privacy to a level that will motivate a response large enough to make a difference. If that is indeed the case, then individuals will continue to be inconvenienced by the aftermath of data breaches, companies will still absorb the resulting losses as a cost of doing business, and governments will persist in taking ineffectual potshots at perpetrators of fraud and other crimes. Thus, the acceptance of increasing violations of electronic and physical privacy will grow and little will be done.

The hope is that the immense cost to individuals, organizations and society at large of repeated privacy abuses is recognized and awareness is raised, not only of the resultant losses, but also that the challenge can be met if there is enough resolve to take it on.

Endnotes

[1] Rainer, L.; J. Anderson; *Digital Life in 2025: The Future of Privacy*, Pew Research Center, December 2014, *www.pewinternet.org/files/2014/12/PI_FutureofPrivacy_1218141.pdf*

[2] Sprenger, P.; "Sun on Privacy: 'Get Over It,'" *Wired*, 29 January 1999, *http://archive.wired.com/politics/law/news/1999/01/17538*

[3] Nanavati, M.; *et al*; "Non-volatile Storage," *Communications of the ACM*, vol. 59, issue 1, January 2016, p. 56-63

[4] *Op cit,* Rainer and Anderson

[5] Lieber, R.; "Identity Chaos, Courtesy of Your Federal Government," *The New York Times*, 15 October 2015, *www.nytimes.com/2015/10/17/your-money/identity-chaos-courtesy-of-your-federal-government.html?_r=0*

[6] If the discussions relating to "net neutrality" are any indication, resolving web privacy and security will likely be even more contentious as the stakes are so much higher.

[7] Chaum, D.; "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," *Communications of the ACM*, vol. 24, no. 2, February 1981, *https://people.csail.mit.edu/rivest/voting/papers/Chaum-UntraceableElectronicMailReturnAddressesAndDigitalPseudonyms.txt*

[8] *Next*, "How DigiCash Blew Everything," January 1999, *https://cryptome.org/jya/digicrash.htm*

[9] Greenberg, A.; "The Father of Online Anonymity Has a Plan to End the Crypto War," *Wired*, 6 January 2016, *www.wired.com/2016/01/david-chaum-father-of-online-anonymity-plan-to-end-the-crypto-wars/*

[10] Khemani, R. S.; D. M. Shapiro; *Glossary of Industrial Organization Economics and Competition Law*, Organisation for Economic Co-operation and Development (OECD), 1991, *www.oecd.org/regreform/sectors/2376087.pdf*

[11] Axelrod, C. W.; "Achieving Privacy Through Security Measures," *ISACA® Journal*, vol. 2, March 2007

[12] Hughes, E.; "A Cypherpunk's Manifesto," March 1993, *www.activism.net/cypherpunk/manifesto.html*

[13] Axelrod, C. W.; "Ensuring Online Data Privacy and Controlling Anonymity," *Proceedings of the Stony Brook University CEWIT 2015 Conference*, Melville, New York, USA, October 2015

[14] *Op cit*, Axelrod, 2007

[15] Boehm, B. W.; *Characteristics of Software Quality*, North Holland Publishing Company, USA, 1978

[16] Axelrod, C. W.; *Engineering Safe and Secure Software Systems*, Artech House, USA, 2012

[17] Segall, L.; "Pastor Outed on Ashley Madison Commits Suicide," *CNN Money*, 8 September 2015, *http://money.cnn.com/2015/09/08/technology/ashley-madison-suicide/*

[18] Adapted from a speech by David Medine, Chairman, Privacy and Civil Liberties Oversight Board (PCLOB) at the *Defining Privacy Forum*, transcript, p. 4-5, 12 November 2014, *https://www.pclob.gov/library/20141112-Transcript.pdf*

[19] The terms "cleartext" and "cyphertext" are used to describe unencrypted and encrypted text respectively. The former can be read directly by humans if on paper or transformed from electromagnetic, optical or other means of recording onto paper, a screen or other readable media. The latter has to be deciphered before it can be understood, and such decryption requires knowledge of a key that will transform cyphertext back to cleartext. Usually the sender and duly authorized recipients know the key, but if the key is stolen or a master key is provided to law enforcement, unauthorized persons can obtain the cleartext.

[20] *Op cit*, Rainer

[21] Ross, S. J.; "Cyber/Privacy," *ISACA Journal*, vol. 1, January 2016, *www.isaca.org/Journal/archives/2016/Volume-1/Pages/default.aspx*

[22] Hackett, R.; "Security Has Failed: Exclusive Preview of RSA President's Conference Preview," *Fortune*, 21 April 2015, *http://fortune.com/2015/04/21/rsa-conference-amit-yoran-keynote/*

[23] Cannon, J. C.; *Privacy: What Developers and IT Professionals Should Know*, Addison-Wesley, USA, 2005