All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

The surveillance society: pros, cons, alternatives, and my view.

I've been thinking a lot lately about the society we are building with regard to surveillance as a way to achieve safety, the well known quote about achieving neither[1], and the direction modern societies and networked environments are going. I have my personal views about such things, but I thought a somewhat less passionate approach might be reasonable. I have started to engage the issue by building this table.

Surveillance pros, cons, and alternatives

There are points for surveillance and counter-points.

Point for surveillance	*Counter-point*
We can prevent another 911 or worse.	This may not be true, but even if it were, this is not the only way; why not use another way? It isn't worth the high price we pay for it.
If it saves one life, it's worth it.	It's not, because it likely destroys a lot more lives as everyone has to live in fear.
If you have nothing to hide / if you didn't do anything wrong, you don't have to worry.	Everyone has something to hide, and everyone does something wrong from the perspective of someone else, but even if I didn't and they didn't, that doesn't mean you should get to see everything I do.
Privacy is dead, long live security.	Resurrect privacy and face your fears. When you give up privacy for security you get neither.
It's better than the alternative.	What alternative have you provided us? Maybe we need to look for some other alternatives.
The system cannot be abused.	There is a long history of surveillance and it has almost always been abused. Your system is no different.
We're the good guys – trust us.	That's what they all say. Trust but verify.
We've caught X terrorists before they acted.	If you spent the same resources in another way, you might have caught more than X.

1 “They who can give up essential liberty to obtain a little temporary safety, deserve neither liberty nor safety.” - B. Franklin (see http://en.wikiquote.org/wiki/Benjamin_Franklin for a detailed discussion).

Point for surveillance	***Counter-point***
The corporations already do it, why tie the hands of the government?	Stop the corporations from doing it too. The corporations don't have armies and police to abuse it.
It's the only technology available to meet the need.	That's not true. Spend time and money to develop other better technologies. Change the need.
We will never be able to analyze it.	Yes you will – unless you are never allowed to collect it.
They aren't after you...	But some day they may be. First they came for the ...[2]
After the fact, it is helpful in investigations.	If you could only use it for that purpose, it might be acceptable, but you can use it for other purposes.
It requires a warrant.	Warrants are given too easily and in secret.
It only applies to non-US persons.	Except when it is abused. Except when it's done by other countries. I'm not a US person!
You're paranoid. Nobody's watching you.	How do you know? It's done in secret. Just because you're paranoid doesn't mean they aren't out to get you. I'm not paranoid, I'm afraid, the surveillance is real.

And of course there are points to be made for privacy and counterpoints:

Point for privacy	***Counter-point***
I don't want you watching me pick my nose.	I don't want to watch you pick your nose either, but it is a price I have to pay if I am going to catch you [doing a bad thing].
What I do is none of your business.	Unless I am in the business of stopping terrorist acts and crimes of violence.
I'm not a criminal, don't watch me.	That's what all the criminals say. You are paranoid, we are not watching you.

2 Various versions are identified at http://en.wikipedia.org/wiki/First_they_came...

Point for privacy	***Counter-point***
The 4th amendment (no unreasonable search)	These searches are reasonable. What you do in public is not private.
Expectation of privacy	You have none – read the papers!
Surveillance has a chilling effect on new ideas and free expression. This ultimately leads to impaired societal performance.	You still have free speech, if there is a chilling effect, it's because you aren't standing up for your rights and speaking freely.
I am presumed innocent until proven guilty, you don't have a right to treat me like a guilty party by surveilling me.	We surveil everyone, no discrimination is involved.
Nazi Germany would have succeeded if they could have had this level of surveillance over their citizens and the resistance.	That's not why they failed. We aren't Nazi Germany. That was 70 years ago.
Saddam Hussein would have ...	If you want to do bad things, you don't need this technology.
It could be used for extortion, to see when I'm not home so as to steal from me, to track me down and kill me, or to commit other crimes.	Only if it falls into the wrong hands. We are only using the technology that bad guys could already use for these purposes.
It's a matter of degree and you have gone too far.	It's a matter of degree and we have not gone too far.
With more surveillance should come more openness, but that's not what happened.	Surveillance without secrecy will only lead to the bad guys avoiding the surveillance.
With computers you can listen in on every conversation and use it against anyone.	The technology isn't good enough to do that. Computers listening to people isn't a privacy violation because no other person hears it.
They will ultimately use it to sell me things I don't need or want.	They already do. There are strict laws limiting government use. Capitalism at its best.
I wouldn't mind so much if I could watch everything all the government officials do.	What the government does needs to be kept secret for your protection.
Information needs to be free.	No it doesn't. In fact, information is often quite expensive. Value increases with exclusivity.
Surveillance leads to oppressive government.	Surveillance leads to safety, not oppression.

I'm sure there are more, and as I get them, I will consider adding them.

Some other notions surrounding privacy and surveillance

The right to be left alone[3] seems to me to be increasingly valuable and decreasingly available. While surveillance can be done covertly and thus "leave you alone" in terms of pestering, the knowledge of its existence can be unnerving and the lack of knowledge of who is watching you when and from where makes it all the more disturbing and creepy.

Some may say that people should learn to "suck it up", and that you have nothing to fear if you aren't doing anything wrong, but in my experience these same people haven't been willing to reveal details about their sexual habits and partners, bathroom habits, birth control, family diseases, and so forth when then asked. It seems that, at least for now, there are still boundaries and people still want some personal privacy.

Pseudo-psychological claims about people seem to me to be problematic. Real people are not always logical or mechanistically oriented. Things that affect people have real effects on their lives and society, and it is not a weakness to be culled from the flock. But on the other hand, folks who make claims without basis in fact or experimental evidence, are really just speculating.

Security folks largely favor surveillance, I think because they think it makes their jobs easier. But I think that attribution for acts is the desired information from a protection standpoint, and that surveillance is not the same thing nor necessary or appropriate to attribution.

The general purpose nature of ubiquitous surveillance is both its boon and bane. It means that if we have the details, we can use it for lots of purposes, some of which we might not have thought of in the inception of the system. When that means we catch a child molester and free the victim after the kidnapping but before harm is done to the child, we are almost all glad that there was rapid access to surveillance to get law enforcement there on time. But when we are planning a "murder mystery" party and it gets misinterpreted as a conspiracy to commit crimes and we get arrested, or when children are surveilled in their bedrooms by school administrators, we generally think that the surveillance was misused and over the top.

It seems almost certain that, for the foreseeable future, surveillance will be part of the world. The ubiquitous nature and extremely low cost of digital sensors combined with the amazing networking capabilities of the Internet and the desire of individuals and enterprises of all sorts to collect information they have legitimate access to, seem to imply that every aspect of the lives of most people, and almost every aspect of the lives of almost everyone else, will be the subject of surveillance. The question then seems to be – What next?

Use control

Use control is and always has been problematic, and perhaps it is the real issue to be addressed. Assuming that surveillance will continue to be deployed in some and/or every way technically feasible, the question then comes down to: What uses should be allowed and/or prohibited, and how will such prohibitions, if any, be enforced? I am going to take a stab at this issue, but don't expect anything definitive.

It seems to me that certain fundamental rights are increasingly considered universal by the global human community, and that they should be considered.[4] These include things like:

3 "The right to be left alone—the most comprehensive of rights, and the right most valued by a free people."—Supreme Court Justice Louis Brandeis, Olmstead v. U.S., 277 U.S. 438 (1928)

4 The Universal Declaration of Human Rights – UN - http://www.un.org/en/documents/udhr/

- Equal protection under the law: *Surveillance and associated uses should be the same for all parties in any legal matter so that if anyone has the right to use or is prohibited from using surveillance results or means, all should be equally empowered or restricted.*
- No arbitrary interference with privacy, family, home or correspondence, nor attacks on honor or reputation: *Surveillance should not be arbitrary, and rights associated with privacy, honor, and reputation should be enforced in its use. For example, leaking embarrassing data from surveillance must reasonably be prevented and punished when it happens.*
- Freedom of opinion and expression: *This seems at odds with privacy in that it seems to imply a right to attain and publish embarrassing information about others.*

There are also notions around a problematic right to be forgotten and an effective right to be remembered (to claim heritage and citizenship, etc.), intellectual property rights, and so forth that play into the mix of issues.

Presumably, these rights imply limits on use of surveillance results. But things get far more complex when technology and the reality of what can and cannot be done technically are introduced.

Technical issues such as data aggregation mean that fusing public information with maps allow you to map out everyone with a gun license, and with access to for-fee databases, you can get detailed photography of the property of everyone that is currently on vacation at a resort of your choosing, get the contact details needed to determine if anyone is home, and then do the more detailed surveillance required to enter their homes and burgle them. You can find out who is using what birth control methods and threaten young people with telling their parents. You can place surveillance on public streets looking into homes and see who is having sex with whom. You can fly unmanned aerial vehicles over private property and land tiny helicopters on roofs with sensitive listening devices. All of this is fairly inexpensive using commercial off the shelf capabilities already available, and it may even all be legal today.

Of course your computer use and other technology use supports this surveillance, with vendors tracking your location and buying habits in near-real-time, parents tracking cars to make sure their children are telling the truth, nanny-cams checking on the babysitter, remote control over houses from cell phones with live camera shots included, keystroke loggers, and all of this potentially available to the end user as well as vendors, suppliers, maintenance personnel, and anyone who has broken into any of these. Increasingly, it is a common and perhaps justified assumption that most if not all hardware devices and software mechanisms sold or provided for “free” to the general public are designed with surveillance built in.

Surveillance is also the basis of a great deal of the protection technology currently implemented within enterprises. This includes such things as virus detection, intrusion detection, data leakage prevention, behavioral anomaly detection, fraud detection, and many other such schemes. The key thing to understand here is that perfect prevention is not feasible today or possibly ever, and that this means we need to detect and react in time in order to reduce the consequences of malicious acts. Inherent in detection today is the ability to observe and analyze content, which is to say, to surveil communication, storage, and processing and selectively stop any of it from continuing. Content and use are thus controlled.

We are in the age of exploring what we can do with the technology we now have and are developing. But we haven't yet reached the stage where we start to decide what we want to do as opposed to what we can do. Can society and does society have the legitimate right to do anything to limit this technology at all? And even if we can and have the right to do so, should we?

It seems certain that some limits will be in place for some time, and those limits will not be technically enforced or enforceable. Rather, laws will be made limiting what who can do and under what circumstances. Those laws will be broken, and prosecutions may or may not happen. Prosecutions will be evaluated by a process that is likely to be highly dependent on culture of the day and of the place. And social change lies at the heart of the outcomes.

Enforcement – civil disobedience – or not

I am not an optimist about enforcement of laws regarding surveillance. I don't believe leaders will stop using surveillance for their own purposes as well as those of the societies they serve, and I don't believe political corruption will end. I don't believe those with advanced capabilities will give them up easily or at all. I suspect that enforcement will be limited at best and unfair, as is the administration of many laws. I don't wish this to be so, but I think it will be. And I think it is important to protest against these things and try to stand up to them.

I don't believe that lying, breaking into systems, leaking secrets, disavowing oaths, or these sorts of things are a valid approach to protesting surveillance. Two wrongs do not make a right. While there is a valid and reasonable way for whistle blowers to operate, cases like the Snowden matter do not, to me, seem to fit that mold.

I am in favor of both strict enforcement of laws and civil disobedience. Indeed, I think that by requiring strict and universal enforcement, we will eliminate laws we don't really want as a society rather than making laws that are selectively enforced based on political, personal, or other extra-legal reasons. I also think that civil disobedience is a valid and appropriate way to challenge what you believe to be invalid or unequally enforced laws, taking as part and parcel of that approach the realistic expectation that you will be jailed and prosecuted. That's what the civil rights movement did, that's what the women's rights movement did, that's what the anti-war movement did, and that's what you have to be willing to do if you want to change things through the non-standard legal process.

Summary of the issues from a logical standpoint

I think the key point is that there are serious issues and tradeoffs involved in surveillance in the information age, and they should be seriously discussed and considered in the decision-making process. I think it is important to have the debate open and public and to get involved. But I don't believe in breaking laws and agreements because you disagree with them. If we want a society with both freedom and justice, we cannot merely ignore laws or break them to make a point. The notion of civil disobedience may seem appealing to some, but part and parcel of that approach is taking the punishments that go along with the crimes.

I think that serious minds differ on the prioritization of these issues and that whatever system is put in place should be flexible in dealing with the changing prioritization by society. I also think that the technologies involved should somehow not be flexible in terms of enforcing the decisions made. That is, the policy should be enforceable and enforced. And that is perhaps a bigger problem than finding the right policy for different situations and societies.

My personal views

My son David asked me, as I was formulating this article, about my views on the conflict between the work that I do and my views on privacy. I was not going to express my personal views in this article as originally written, but I think it is reasonable and appropriate to do so. Something about being responsible implies sharing your views.

I have different views that are in conflict. They are represented to some extent by the tables above, but they are more visceral and less logically oriented than the tables belie. I do view the issue as largely a question of use. For example:

- If you tell me I cannot use a surveillance device on my property and record what goes on, I think you are violating my property rights.
- On the other hand, when it extends beyond my property, like surveilling the streets around my house, putting up a tower and collecting signals from outside my property, and so forth, I think that is going too far, largely because it means that you could watch what goes on in my property, and that's a violation of my property rights.

In the context of the Internet, I think that anything I generate or do within hardware or software I buy should also be considered my property and be subject to my exclusive control. It's the same kind of property right in my view, and should extend to me wherever I am.

Commercial issues

Services are a trickier domain. There are two general areas at issue here. (1) when I pay for it and (2) when someone else does.

- I think that when I pay for Internet service or any other service, the deal should allow me to pay for the costs plus profit and that the other party should not record anything about what I do other than as necessary for billing. In the case of services where the price is fixed and usage independent, no usage information should be allowed to be recorded at all by the service provider. And as soon as I pay the bill, the records required to get the bill paid on the service provider's part should be destroyed.
- On the other hand, when I get something “for free”, I know as should everyone else, that it is not really free. I should always have the option to pay what it costs plus a reasonable profit rather than getting the service for free. But if I choose the “free” option, I should be clearly informed of all uses. To be clear, when I say “all uses”, I mean it. You are purchasing use of my information for a fee – that fee being the service you provide to me. At any time, I should be able to stop paying and stop getting served. And that means that I control all of my information. The instant I say stop, the information must get purged. And I mean everywhere. If you say you are selling its use, that's fine, but you have to list all the buyers, and they have to be subject to the same terms and conditions. And I should be able to say yes or no to each and every use if I so desire.

How about my convenience? Many providers tell us all that the data they save about us helps them serve us better. No problem. Leave my data with me and provide the software on my system to be run under my control that allows you to serve me. Let me control everything about it including what is collected and preserved for how long, and let me delete whatever I want whenever I want with no control or knowledge by you. If I choose to allow analysis to be

done with my data and/or sent to you, that's fine. But it should be under my control. If I want to charge you for the use, I should be allowed to, at any rate I choose, changeable at my sole discretion. This also implies that my system must be able to control such uses, or that usage by your programs running in my systems be limited by law with punishments for violations.

Now let's talk about defaults. I believe in “default deny and destroy” when it comes to information about me.

- The default should be “no you cannot have or use it”, and permissions to gain access should involve a hand-written signature.
- Revocation should be something I can do with a single click of a button.
- All of the extant permissions I have granted and the payments I receive for them should be readily available to me at any time in a single comprehensive interface that is easy to use and clear to the least sophisticated users among us.
- If I want to change the price, I should be able to do so immediately, and to the extent the price then becomes something other than services (e.g., money), as of the moment I change the price, the new one should come into effect.
- The vendor should have the same right to change the price as I do, except that I require notice because I am not an operating business, just a person. Rather, the vendor should be required to meet my price or destroy the content, just as I am required to meet their price or stop using their service.
- Terms should be simple and standardized with no exceptional language permitted. For example: “You get free use of our Web server to post your content and we get to sell advertisement space on top of that content.” Obviously limited additional detail may be required through a drill-down of some sort, but it should be just about that simple.

To review – permission hard – revocation easy – default deny – offer and accept bargaining.

The punishment for violation is another key issue here. If you have small punishments or hard to attain judgements and enforcement, none of this will work.

- My view is that the punishment for violating my rights should be very high. Let's say $1M per instance (perhaps for each bit you have that you shouldn't), with the presumption favoring the plaintiff (me or more generally the individual) and all costs borne by the loser. The goal is to make the punishment so high that companies and individuals won't cheat.
- I want law suits with adequate basis (whatever that is). To assure that things go smoothly and quickly, all of the information required to sue and defend should be immediately available to the consumer as part of their interface to control use. Failure to provide all such data constitutes a cause for summary judgement against the defendant, which is to say, if you hide a use and get caught, you immediately lose the ability to defend yourself. It was accidental? Get out of the business. Accidentally forget, but don't accidentally remember.
- Enforcement should be by independent randomly selected auditors, paid for by the industry, but without their advanced knowledge. Stand and deliver right now.
- Any citizen wishing to do so should have access to audit on their own as well.

This should be part of the cost of doing business with other peoples' information. And of course anyone should be able to sue using existing legal means if they don't think the enforcement works properly. If it seems expensive for those wishing to take and use personal information in anything but the most above board way, you understand me correctly.

Control of content should be inexpensive and easy for those who are legitimate and expensive and hard for those who are not.

Government issues

As a fundamental, I think that surveillance and the use of data from all sources for any and all things is undesirable. Government, because of its enormous power over people, should be limited and closely watched. The long history of government is that less transparency leads to more abuse. “Power corrupts...”[5] And you cannot believe what government officials tell you.[6] But surveillance of some sort is necessary for the legitimate business of government. While it may be impolite to read others' email, you cannot reasonably expect the government not to do so under some circumstances. The question is: “What circumstances?”

I have long maintained and believed that oppressive societies may not be internally overthrowable if they are able to adequately surveil their citizenry. This applies regardless of the system of government. The problem stems from the fact that people are not perfect and there will always be something that can be leveraged against the individual by the government. Leverage may be in identifying illegal acts and selectively prosecuting them against the enemies of the state, but it need not always be done that way. Extortion and bribery work very well in many cases, and even without such extreme acts, most people can be diverted from their course against the government by other things. Suppose I got you a good job doing something you always wanted to do in a great place and where there are lots of things to do with your time. Would that tend to reduce your revolutionary bent? Likely it would for the vast majority of such potential future leaders. My point is that the different ways of changing peoples' approach to the world do not require direct action against them in most cases. With enough information properly processed, we can change the world one mind at a time, and we can change the conversation en masse. Information operations against the citizenry is really the worst case scenario in my view, it happens all the time, and with more surveillance this works very much better than with less of it, because we can craft messages more individually and get feedback on the effects of those messages on the individuals.

At the same time, it is hard to argue against catching child predators who kidnap children and get caught on cameras and then tracked down. The apparent Israeli killing of a PLO leader in a hotel[7] and the demonstration of the use of surveillance to track down the parties involved[8] is, in my mind, an example of the possible benefits to law enforcement (and deficits to those in covert operations). I recognize that spying against, and surveillance on, those from other countries is a part of what secures each nation from others and that without such efforts, the

5 "Power tends to corrupt, and absolute power corrupts absolutely. Great men are almost always bad men." John Emerich Edward Dalberg Acton, first Baron Acton (1834–1902). The historian and moralist, who was otherwise known simply as Lord Acton, expressed this opinion in a letter to Bishop Mandell Creighton in 1887: per http://www.phrases.org.uk/meanings/absolute-power-corrupts-absolutely.html

6 Remarks As Prepared for Delivery for the Center for American Progress Event on NSA Surveillance: http://www.americanprogress.org/wp-content/uploads/2013/07/7232013WydenCAPspeech.pdf

7 http://www.nytimes.com/2010/01/30/world/middleeast/30dubai.html?_r=0

8 http://www.youtube.com/watch?v=kzzzTtpo8AY

security of all peoples and nation states come into peril. The question comes down to how we can gain many of the benefits of use without suffering many of the harms associated with abuse of these technologies.

I think the solution is private and local ownership of all surveillance mechanisms within each country and at every level of granularity. Sharing should be legally and technically prevented in large quantity, but supported and legal in small quantity for directed purposes.

- If and when something is to be shared it should shared by physical transmission (hand physical media with the specifics of what they asked for) and require a court order.
- The court order should be made public no more than 90 days after issuance, and always subject to counterargument and appeal processes before being acted upon.
- Destruction or failure to retain content once ordered should be punishable by jail time.
- Voluntary sharing should be permitted as long as all parties with property rights are informed and explicitly consent to the specific act of sharing. You need to get my signature on a piece of paper granting you permission to share each specific piece of data, and I must examine each piece of data before consenting.
    - To be clear, that means that even if I consent on entry to your facility to being recorded, before you can reveal it to any 3rd party, you need my written consent to reveal what you recorded, or a court order to do so.
- I think that the proper granularity is at the level of ownership and property rights. A building owner may have rights for the hallways, but each leased space is under the control of the lessee. My house and land, I should control. The city streets and parks should be controlled by the various departments of the city. Outside of cities, counties have the responsibility. All states consist of counties, so no state level surveillance should be allowed except for state buildings and properties and other similar lower level of granularity locations. At the national level, again, Federal buildings and lands are presumably Federal responsibility, but nothing else inside the country.

How does that work? If you are at a state agency and want a record collected by the county, you need to request it through a formal method that is subject to objections and appeals, and you may not have access without that process. Expedited orders from judges can happen of course, under exigent circumstances, but even then, the information cannot be retained after use or used for any purpose other than the specifics of the court order, which must be as narrow as possible for the specific need. If, in the process of chasing down the kidnapper the law enforcement official happens to see a murder taking place, they should certainly be able to go to the judge and ask for appropriate search warrants to proceed with the other issue.

That's really the whole thing as far as I am concerned. Surveillance? Sure, go to it. All you have to do is get court orders for each entity you want information from for each case, narrowly defined, and be handed only the relevant information from that entity, subject to objections and revelation of the facts of the surveillance within 90 days. Wholesale? Not likely. No blanket warrants, each has to be specific to the specific case. Get critical information quickly? Sure. Within an hour of a request, we can probably get you anything you want. But getting data in large quantities takes perhaps hundreds of thousands of officers with warrants from thousands of judges, with everyone knowing what you did and appeals along the way.

The point here is that **ANY** is not **ALL**. Government needs to have access to **any**thing, but **not** **every**thing.

In simple terms, some safety should be sacrificed for a great deal of freedom. But how much?

A final personal note

I have found myself somewhat stifled by fear of reprisals for things I might express. Starting when I first did research on computer viruses, I was afraid that someone in authority might decide that by eliminating me, the nature of viruses might be kept from general knowledge. My response was self-defensive in nature. I revealed essentially everything I knew that didn't involve a specific confidentiality restriction, and did so as soon as I could so as to minimize exposure. Such restrictions only ever applied to facts regarding specific organizations, and nothing of general interest or utility was ever delayed for long.

Between that time and the last several years, I always did the same thing. Of course I never revealed anything classified, although some of the things I revealed ended up classified later by others. I suspect, but certainly cannot prove, that my ongoing openness regarding protection issues and their exaggeration, misstatement, and mischaracterization is the reason I was ultimately separated from Sandia National Laboratories (who said nobody got fired because of 9/11). When the national laboratories were seeking monies by trying to frighten the government decision-makers, I was allaying select fears that I thought were not justified.

But recently, after I was funded to do some government research, I have felt increasingly like I should not say what I think, particularly in regard to this and related issues. Now there is some validity to this notion. For example, people with clearances are not permitted to read the material from Wikileaks that may or may not be classified, or similar potentially classified information released by other sources. It seems crazy that people who are cleared are not allowed to read what people who are not cleared are allowed to read. Why should people you trust not be able to see things that people you don't trust already know? The answer I have been told is that if people that have clearances read the material they might comment (as en example) that it looks like classified documents (or doesn't). Of course this is ridiculous on its face because the specifications of what classified documents are supposed to look like is unclassified and openly available. But the rule is the rule, so I follow it, while making it clear that it should not be the rule and it only serves to make cleared people less informed.

In addition, some of the events in the media have resulted in explicit statements by funding agencies not to comment or talk to the media on issues related to the research we are doing or the issue associated with it. Now don't get me wrong. I wouldn't talk to the media or anyone else about anything that is client confidential, regardless of whether the client is the government or anyone else. As a general rule, I don't reveal client names, even though it would probably get me more work if I did. So I am not being oppressed or otherwise restricted from saying anything I might otherwise say. But still, there are other things.

This article was delayed because I was (and still am) awaiting a decision on possible membership in a national-level thing (whatever that thing is/way is irrelevant). The thing is unrelated to the issues of this article, and yet, I have the notion in my mind, that publishing this article might hurt my chances. I don't know where I got the notion, and certainly nobody and nothing involved in the process indicated any such thing. And yet, somehow, I have this feeling that it might have a negative affect on my selection in the process.

The reality is that I don't have a realistic chance of being selected regardless, but that's not the issue. The issue is that there are psychological effects of feeling as if “they” might be watching. One reason I decided to publish this article now is to counter that feeling in myself. The other reason is that I think I have been thorough enough now... I hate to miss things.

Summary

To be clear, my personal views are not consistent. That's the nature of the way I think about these issues and why they seem to me to be complicated and somewhat unclear. I hope that the same is true for others. This is not a simple issue and should not be dealt with in a simplistic way. That's my view.

I should also point out that my view is unlikely to be widely embraced. It is, in some ways, hard over. And in the meanwhile, the world continues down the path toward global ubiquitous surveillance – a.k.a. the Internet of things, total information awareness, or whatever you call it.

- It means we will be able to tell when diseases are spreading by the search and purchasing habits of Internet users, and we will also be able to tell when you are not really sick but just taking the day off.
- It means you will be able to find the best price for your birth control, but it also means that we will know who you are sleeping with, when, where, and what positions you use.
- It means you will only get advertisements for things you are interested in buying, but it also means you will buy more things you don't need or want after you have them.
- It means the government will be able to hunt down people who commit crimes, but it also means that politicians will be able to hunt down and kill political enemies.
- It means that some terrorists will be caught who otherwise might have gotten away with it, but it also means that you are more likely to be enslaved by your government.

My view is that all of those things and more are coming to pass. And it is my view that unless the people of the world act to stop it, this will be our future for a very long time to come.

And yet, I continue to work in the security space where, among many other things, I help people use surveillance and analyze results of surveillance of various sorts in order to seek the truth and protect their interests.

Returning to my professional perspective, I believe that thoughtful people who are given the chance can come up with better solutions than massive surveillance can and will do so. The challenge is giving them this opportunity. Surveillance and “big data” approaches are popular today, and the whole field of information sharing and the infrastructures being created to facilitate it are part and parcel of this approach. While I generally support understanding and applying these approaches, where appropriate, I also think there is a real need for the loyal opposition, especially in research, and for alternative approaches to be developed and applied. Unfortunately, research is not funded that way, at least today. The popularity of big data and the vision of computer intelligence saving us from ourselves seems all the rage. But that too will pass. Intelligent computers are still a very long way off.

I hope that you will consider alternatives and identify new approaches better than those I have outlined. And I hope that as a society and a world, we can avoid the future that massive and unfettered surveillance and analysis portends.

