Unintended consequences

We can't deter or prevent many of the activities we wish we could deter or prevent in the use of computers, for some very good reasons (there are known theoretical limits on what can be done in general purpose computers and human behavior is not really all that controllable) and some very bad reasons (computer programmers don't like to do the hard work of engineering solutions that work properly under known environmental conditions and we don't bother to do the hard work to understand how to control human behavior better).

An unintended consequence of not being able or willing to deter or prevent bad things is that we are forced to try to detect and react to them. Of course we can't really do that well ether – in fact we don't even do that as well as we prevent things. But as an industry, the computer security companies can generate ongoing revenues from detection and reaction that they cannot get from prevention, so they sell the services for eternal fees rather than the products for fixed fees, and they make money while consuming their share of every dollar spent and never really get it right.

An unintended consequence of detection and reaction instead of deterrence and prevention is that we move increasingly toward a surveillance society. We have television shows that show how the cameras benefit us all and show silly things that people, cars, and animals do, and it helps to humanize the ubiquitous surveillance. Because we cannot change our society to a civil one, we turn it into one where big brother is watching and you better not shout or cry, the private companies and governments that own all the surveillance can show you why – on video tonight.

An unintended consequence of cowing the society by surveillance and projecting the image that all of this surveillance is really just fine an in your best interest, is that when I watch the executives who forget they are being watched, and I see them with their new mistress, I can extort money from them or sell the videos to the highest bidder. The effort to eliminate the crime moves the crime to the population that is supposed to be detecting it.

An unintended consequence of increasing the surveillance and the number of trusted parties that have access to all that surveillance is that we no longer know who is watching or who can really be trusted. But since we can't tell anyway because the bonds of trust and community are gone, it doesn't matter, so we can outsource it all and save a lot of money. After all, what's the real difference between a worker from China and one from Europe?

An unintended consequence of outsourcing – unintended by those who make the decisions that is, not by those who take advantage of them – is that governments, organized criminal groups, and corporations can launch various kinds of information warfare, criminal activities, or competitive activities (which may all be different names for the same thing) that otherwise would be unsuccessful and expensive to do. The criminals are gaining the advantages of the efficiencies of the Internet and using our grand new capabilities against us.

All of this stems from a very simple and, I think foolish, mistake made long ago and repeated day after day. It's the mistake of giving up on building more secure open computing platforms. The intended consequence of this article is to start the discussion back up – yet again – and get to the only real solution that will ever work if we want a free society with networked computers. Deterrence and prevention – the only real option we have. But how do we do this?

Deterrence is something we have discussed. It has to do with perceptions of people, and as such, it is in the realm of security psychology. This is an area we don't study enough, and as a result. we rely on fear, uncertainty, and doubt as the cornerstones of our efforts at trying to achieve morality, desired behaviors, and compliance. Is there any wonder, that this will never work? Fear results in compliance – sure enough – and revolution. People who are afraid will typically engage in fight or flight, neither of which is very good for making people more comfortable with being good and doing right. Instead they will get the sense that they are at odds with security and fight against it – in underhanded ways. You will get malicious compliance, challenging of rules, people posing for the cameras, and turning in of people who don't deserve it.

The path to better behavior in most people comes from having them believe that the things that security does are in their own best interest and done with their understanding and support. Security from on high will not achieve this. Sensible security that engages the people who have to do the work every day is necessary in order to have it work. We need to engage in real discussions of the issues at hand with the people who have to live with it. If we don't, the plan will fail. The best way to deter bad acts is to make most people not want to do them.

But no matter what we do, at least for the foreseeable future, there will remain bad actors and they will do bad things. That means that, if done well, we will have a relatively low noise environment where most users are doing the right things most of the time and re not getting anywhere near the boundaries where we need to differentiate their behaviors from bad behaviors. I sometimes used to tell my kids that when I say to stay out of something it does not mean to come as close to the edge as you can get, because I will treat anything that requires me looking more deeply into it as breaking the rules. The separation of good from bad by as much distance as possible is a very important thing to do, and many bad actors specialize in trying to stay near the legitimate to avoid being noticed.

To address prevention in an environment where people are behaving well for the most part, there is a need to understand the options. At a top level, the technical options are; (1) separation, (2) transformation, and (3) filtering.

