All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

How to destroy security – by 'enhancing' it

It is no longer possible to have a memorable password that you use to do anything useful on the Internet. No, we have moved on from that to where the only way you can use a computer usefully is with another computer. And to use that computer, you have to have another computer. Which is to say the circular IT 'economy' has increased the dependency on the big firms to the point where they can now take full control of the information world. And they largely have. All in the name of 'security'. I hope we are proud of ourselves in the security field for destroying computing by over-controlling it.

So-called democratization

I have long heard folks talk about democratization brought about through the Internet, and indeed, in the early days of the Internet, democracy was well serves, as was freedom of speech. But as 'security' pushed toward using the Internet as an intelligence platform and sought to lock down all activities and content, as is the way of all such things, it became so 'democratized' that it became a means to achieve a combination of anarchy and autocracy.

Now this may seem a bit ridiculous on its face. How can it serve anarchy and autocracy? Simple enough. One leads to the other.

- The claims of democratization are almost uniformly a desire for anarchy, where nobody is in charge of anything. But what really happens is those motivated toward using the capacity for concealment and anonymity associated with the freedom of democracy move toward the development and use of anonymity and concealment, and the more important it is to them the further they move there. Technocrats support them for money, in many cases ignoring or embracing the criminal nature of those who are at the extreme end of motivation for concealment and anonymity. Of course we hear through publicity about freedom fighters and the oppressed who need this anonymity in order to get their cry for help out. But there are far more criminals in the world with far greater resources than the truly oppressed. So we get more criminals more successful and as they gain more resources, they take control of more of the 'legitimate' enterprises, and we have massive criminally owned infrastructures.
- The sincere cyber-'security' folks, of course, seek technical solutions to social problems, and thus they find ways to break the increasingly effective and well funded technology of crime. They could seek really smart ways about it, but usually not. They pick the 'easy' way, not that the 'easy' way is all that easy. Their path is mass surveillance. Of course we tell ourselves that it's not really surveillance if no person see it, and we emphasize so-called 'privacy' under the essential claim that even though the computers can see and analyze all we do, other people don't see it, so it's really private. The autocrats love to use these distractions because by being able to see anyone any time it's almost as good as seeing everyone all the time, perhaps even better, for a while. But only because of their limited resources. But wait. What if we get more of this technology and keep working it to the point where we can 'watch' almost all of the people almost all of the time, in the sense of detecting what we care about?

So the autocrats use the anarchists as motivation for the gullible public in the middle to ‘fight crime’ (which they largely own) and ‘save the economy’ (which they largely own), to take more of the wealth and more of the ill-gotten gains, and ultimately change the laws so their acts are no longer crimes.

So-called free speech

Free speech in the age of the Internet is nothing like free at all. It’s downright expensive. Of course you can send an individual message to anyone, all you have to do is pay for the basics. Internet access, a device to connect to it, the time and attention to learn how to use it, and of course allowing the providers to control it all. Sure,m you can use he library for it all, at the cost of inconvenience. Until you have to show ID at the library and they keep track of which computer you use and when. Then the records can be associated, and of course everything is attributed to you. But you only have to pay for the trip to the library, which you can walk to in many cases. However, because anybody might steal your password, we need to add multi-factor authentication for ‘security’. The net effect, you can no longer just go to the library and send an email, because you need to own a device – and likely to use the device you have to provide a fingerprint or facial scan. So it actually costs more (such some more money out of us please) AND assures that your every move can be tracked and associated specifically to you.

But of course you can use encryption to get around all this, perhaps by using an encrypted social media app (which you authenticate via email in order to gain initial and ongoing access). OF course the encryption keys you generate yourself ar not good enough for the browsers and email clients, which only trust you as you if they tell them so. So for ‘security’ we cannot trust self-certified certificates, but only the ‘secure’ ones run by big companies and controlled by government. So in order to still use these techniques with effect, you either have to work harder and harder and be less and less ‘trusted’ by everyone else who uses the highly supported tighter and tighter attribution and definitive surveillance for ‘security’, or you can just go along to get along and reduce your burden to the current MFA and built-in mechanisms of whatever the big tech companies hand you.

But that’s ‘free speech’ in the small. Free heavily surveilled speech analyzed by the good folks from computer ‘security’. Keeping us safe by protecting us from the terrorism of emailing each other, which of course can be used to coordinate terrorist plots. Except of course the bigger plot to take over everything which supports terrorism to some level to keep the fear going to justify the ‘security’ (control) enhancements.

Big ‘free speech’ is what happens when we allow people to communicate to lots of other people. And that is closing in on dead.

Email in the name of spam

So now that we can send and get encrypted email by using multi-factor authentication and paying for an add-on device and a set of services, or we can use ‘social media’ which does not support end-to-end content encryption at all, and is built to ‘monetize’ everything we put into the system, with its massive advertising base to make it ‘free’ for us, except of course if we want to use it at larger scale, in which case there is a fee… of course they have to stop the emails from getting through.

Come the ‘spam blockers’. In the name of ‘security’, and because the bad guys are using email and social media and text messaging and everything else to trick us into doing something that lets them take over our bank account, computer, digital device, or whatever; we need to detect and block ‘bad things’. Of course we would try to make the platforms we use more effective at self-protection by other controls, but let’s go the easy way (and the one better for the autocrats) and start scanning email content for ‘bad things’. Of course this has been around for a long time, and the anti-spam fanatics don’t care who they hurt as long as they aren’t bothered by people communicating with them except the people they already know. So now, if you want to communicate to more than a few people at a time, you will likely start to encounter the spam blockers. How do you get around them? Take a guess…

Yes, that’s right. You sign up to a service that charges you more and more as you communicate to more and more people. And you get less ‘security’ blocking because you come from a more popular place. They are ‘trusted’ (not necessarily for any good reason) and they charge a fairly hefty fee (which the market will bear for a while) to allow you to send more messages per hour than the other players. Just to be clear about the thresholds today, about 100 emails an hour is what you get per account, and of course by having more accounts, you can send more, which means it’s about the money, not the ‘security’ which is what they usually claim it’s about. If you go to something like a groups account, they can send out 25,000 emails within a few minutes without a problem, and they will let you do it, after you pay them enough over a long enough period, until someone complains…

Of course you can use social media, but then your 10,000 connections really only gets any individual message you send in front of a few hundred people. So you cannot run a systematic campaign, unless you pay for a special service that lets you communicate with more of them. Pay more, get more.

Free speech for the rich and powerful

Of course if you have the big bucks, you can get lots more. At some level, you can pay for more of the commercial services, and as you pay more you get more. To become popular you can create lots of accounts, or have someone overseas do it for you on the cheap, and build up thousands of fake fans. Of course the technology doesn’t know they are fake, so you have the social proof to be popular, and once you are popular, lots of other folks want to listen to you. So why doesn’t ‘security’ stop these fakes? Because it pays the social media companies to seem more popular, they fake it till they make it, and they let you do it if you pay them. They have shown some ‘security’ capacity to stop it, when they want to, which means they allow it when it is in their best interest. It’s financial ‘security’ for them to not have too much ‘security’ to help you.

If you get richer and more powerful, eventually you start to control larger assets, which means you get to communicate, or stop others from communicating, in massive quantities. Money buys speech, and more money buys more speech. However, if you try to speak too freely in major media these days, you will be walked out of the door by ‘security’. It appears that the major media in the US have been largely taken over by the ultra-wealthy and they are being threatened by the folks trying to become autocrats, and they are bending to the will of the future autocrats by taking speech away from those who disagree with the people in power. That’s how the rich and powerful got there and how they intend to stay there. And ‘security’ is the tool they will use to do it.

Come AI

I have long said that one of the key reasons the Nazis couldn't hold Europe was that they didn't have the technology to surveil and analyze all the folks who were against them. And for a while that remained true even in the Internet era. But the times they are a changin'.

AI, and the associated analytical disciplines enabling and supporting it, have reached the point where this is no longer true. Thanks to 'security' AI has increasingly been used for better and more precise surveillance that tracks individuals everywhere they go and enables fusion of location data, financial data, communications data, psychological profiling, association data, physiological data, and more to allow everyone using the Internet or moving about 1st world countries to be more or less individually tracked, analyzed, and detected in terms controlled by those who operate the surveillance systems and fusion centers. They use it to take money from us all right now, and they associate us into networks they map to identify key individuals. But because it gets right down to the minutia of everything you say or type, every facial movement, every transaction, your health records, what you own and value, how you feel, your psychological and biological traits, and even your genetics if they want it, they are pretty much able to do what the Nazis were never able to do. And the newest of these technologies, turning brain activity patterns into literally spoken versions of what you are thinking, makes it all the harder to escape the sensor world we have built. To keep us safe, these will all be used for 'security', and many of them already are.

You can use AI to build your enemies list, and if you are rich and have access to lots of records (have you been watching the news lately?), you can use AI to automate your enemies list at scale and start to brutalize them. You can select your allies at the individual level, push information out to get responses, and based on those responses destroy the lives of the people who would oppose you. That's today.

Ignorance is bliss – until it's suicide.

One of the longstanding claims about technology is that it's a two-edged sword. It can be used for good or evil. But the ignorance of the populous writ large, enhanced by the deprecation of education over generations, enhanced by the divide and conquer strategies that are working so well, has brought us to the point where a major shift in society is taking place right in front of us. Our ignorance, brought on in part by generational time frames between these sorts of events, enhanced by intent of those wishing to enslave us all, has hopefully peaked, but I am unconvinced that it can not go further or that it is not too late to stop the autocratic outcome that will last because the technology of 'security' has ultimately been twisted away from the well being of the people toward the control of the poor by the rich and the increasing gap in the middle.

Conclusions

It's not that technology is a two-edged sword. It's that those wielding the 'security' swords are sharpening their edge while dulling yours.

We build the technologies for various reasons, perhaps in many cases just to show that we can understand it all, but it ultimately becomes part of 'security' under the name of keeping us from harm by whatever they find we fear. When what we should fear is 'security'.

Security: Protecting the rich against the poor and the autocrats against the people.

