Fred Cohen & Associates - Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Why are we so concerned about governments getting our data?

I have been reading a lot lately about how governments want to read encrypted messages sent through large-scale services like Gmail and Yahoo mail. Governments around the World want the keys to read the messages, and individuals throughout the World are concerned about their privacy from government surveillance. But what people are concerned about seems strange to me. It's not that they should not be concerned... they should. But if they want the right outcomes, they should be concerned about the right things.

What is the real concern here?

I want to start by saying that this problem seems to me to be very similar to the things I hear from the US political system, which are also strange to me. For example, the oft repeated claim to the effect that we must not increase income taxes on the rich because they will be hesitant to hire more people if they have to pay more taxes. Of course this is simply ridiculous. Higher taxes mean that, effectively, employees are less expensive, because you don't pay income taxes on what you pay employees, all of that money is deductible and reduces your net profit. If you can get more than a dollar back by spending a dollar on an employee, you end up with more money at the end of the day, regardless of the tax rate. But if you are investing by hiring the employee, then you are betting you can get more back later by spending more today. In that case, instead of paying 50 cents to the government in taxes, you are spending a dollar on the investment, and if you get more than the dollar back later, you pocket the difference (less taxes), and you don't give the 50 cents to the government today.

What does this have to do with the privacy discussion? Everything! Outcomes in government are largely dictated by the discussions that take place – what factors are considered and how they are weighed against each other. By creating and debating false arguments, real issues are avoided, and outcomes are based on false comparisons. The debate surrounds a false choice and the choice made seems like it's not as bad as it might be if we were thinking about in in different terms. And that is my real concern here.

Perspective vs. reality in the privacy debate

In the discussion of privacy, the discussion is largely surrounding whether keys to read encrypted content, which the provider has or has the ability to have, should be given to governments. The positions typically taken are that this will stifle free speech and destroy the privacy of the people communicating. But this seems to be to be a set of false arguments.

Free speech means, in essence, that you can say anything you want and that the government cannot arrest you based on what you say – within some limits. But keys to read encrypted content don't in any way prevent anyone from saying or writing anything they want to anyone they want. They don't change the laws regarding freedoms to speak your mind. At most the effect is to know that what you say will be known or knowable to more people – which is what free speech protects.

The free speech argument usually then follows into the realm of inhibiting speech by making it less private. It has a “chilling effect” on speech by knowing that others, including those who work for the government and those they reveal it to, will know what was said. They may feel as if they don't want to communicate because their communications will not be private. But this is not a free speech argument, it is a privacy argument, and should be discussed in those terms in order to properly understand it.

The privacy argument is also problematic. Since Google and other providers already have the ability to read messages if they want to, privacy depends on the actions of the company. Why should anybody trust a company? Motivated by money – and with no legal obligation to preserve privacy other than contractual obligations that it makes privately and can change privately, a company and its employees may read the content at will, and likely even alter contents. A government – motivated by the population it serves or at least rules over, has no financial interest in reading anyone's messages.

That is not to say that political issues in government are not real. They are. Governments have broken privacy promises before, and the US government apparently does so all the time, while many other governments simply make no such promises. Privacy is a real issue, but it is not addressed by stopping governments from doing what they will. It has to do with people holding their own keys and protecting their own privacy. Similarly, corruption of content and forgery of records is a real threat, and it too can only be defeated by individuals protecting themselves.

The technical solution

At one time, “PGP”, which stood for Pretty Good Privacy, was indeed pretty good at protecting private content of individuals from anyone other than intended recipients being able to first view it. If the sender and recipient did their jobs well, the system worked well. And it could work still today. But unfortunately, it is reasonable to say that the privacy ship has sailed.

- Senders and recipients almost never do their part of the protection job well enough to be effective against the real threats that exist.
- Software vendors cannot be trusted to provide software that governments and others cannot access and bypass, making privacy even harder for almost everyone.
- Service providers have financial motives for not protecting privacy, have proven to be easily swayed by governments, and have not proven trustworthy in this arena.
- Operating environments are full of security holes and increasingly subject to updates that may introduce intentional protection bypasses for governments and others.

Conclusions

Why do we worry about governments getting our private data? Because they have abused it in the past. But so have companies, including providing it to governments under legal mandates and in some cases even without such mandates. If we are going to trust someone other than ourselves, companies are far worse candidates than governments. But in truth, even the best of us are likely to depend on others in one way or another, and transitive trust has proven faulty again and again. In short, privacy is dead, and if you are forced to trust anyone or anything, governments are apparently the most trustworthy of the poor choices.

