Julian Assange on the surveillance society - abriged version of the first part of an interview with Seung-yoon Lee, CEO and Co-founder of Byline; full text at https://www.byline.com/column/3/article/83

"Western civilization has produced a god, the god of mass surveillance. How is it like a god?

If you look at most definitions, a god is omnipresent, omniscient and omnipotent. In particular, god knows when you are doing something that you shouldn't be doing and whether you are playing according to god's rules.

The conception of national security agencies and mass surveillance is that the overwhelming majority of communications are surveilled upon.

We've increasingly become accepting of the surveillance that exists at all levels of society. It's hard to escape from that in any traditional way.

Over time, there will arise an acceptance that this is simply how society is -- as has already arisen with other forms of surveillance. At that point, society develops a type of self-censorship, with the knowledge that surveillance exists -- a self-censorship.

Historically, the spread of the Christian church is an example of how that conception of an omniscient being that monitors any deviation from the rules, is powerful and has an effect on people's behaviour - enough of an effect for the Church to expand and thrive. If you read about people reared as devout Christians, who were constantly terrorized as children about committing a small sin and going to hell, it really does dominate their life and it dominates their behaviour, and often in a very bad way. As a group this makes them conform to things that perhaps they shouldn't be conforming to. I think there is an extreme danger here, it changes societal behaviour and makes people conform in an unhealthy manner.

There is an extreme danger here, it changes societal behaviour and makes people conform in an unhealthy manner.

In the end it doesn't matter whether Google is a completely willing participant, a partly willing participant or a not at all willing participant of mass surveillance. All that matters is that it is Google's business model to collect as much information about the world and people as possible and store it and index it and compile virtual dossiers on everyone and predict their behavior, and sell it to various organizations and advertisers and so on. For any organization that does that and is based in the United States, the U.S. National Security Agency and other intelligence agencies will make sure that they get hold of that information. It's simply too easy to do so and too attractive.

Because the Internet globalizes information markets, that means there is just one information market.

For any particular communications service there is going to be a market leader, and then some company that has about 10 percent, and then the rest are insignificant. The National Security Agency only needs to go after and compromise the market leader and maybe the second organization to get nearly everything it wants, and capture most of the population.

If you have any popular service, that popular service becomes a very attractive target. Millions or tens of millions will be spent on compromising that attractive target, and how many companies can stand up to that?

In 2013, the U.S. Security Agency spent over $300 million compromising security companies, by buying parts of them and by bribing employees. That is not including money spent on technical attacks as well. How many people can stand up to a million dollar bribe plus threats? How many engineers can stand up to that?

You go after the individuals. Go after some engineer or system administrator. Or you go after the libraries, the other programs that are used to build encryption programs. Can all those people stand up to million dollar bribes, threats, computer hacking of their personal machines? No, not many -- that is the problem. To properly protect an organization, you need technical defences, you need human defences, political defences, legal defences, all of these. And only one of these has to go wrong, and then you have a backdoor into the system. That's the problem.

The purpose of intelligence gathering is to understand what is happening and then to create a plan in response to what is happening. We have two loops. In one, a country like Ecuador, its political leaders are observing their environment, thinking about their observations and creating a plan and enacting the plan. Having enacted the plan, they observe, create a new plan and act on it. The National Security Agency and those kind of organizations are doing the same thing. They are observing what is happening in Ecuador. They have almost total observational power. But they still need to understand what is happening from these observations and then create a plan. All of this takes time. But if the time for organizations and smaller states to understand their own environments and act on it is shorter than it is for large bureaucratic states like the U.S., then by the time the U.S. has worked out how to subvert the Ecuadorian electoral process, for example, the campaign decisions have already been made and the situation has moved on.

But in the end, I think it really comes down to small, fast organizations with really bright people in them, versus very large, almost Soviet-esque, secretive government

organizations. Now, secrecy breeds incompetence because where there is failure, failure is kept secret. Also, the best and the brightest don't really want to go and work for a big bureaucratic secret organization where their talents can't really shine because it has to be kept secret. If you look, for example, at TOR co-founder Roger Dingledine, a very bright computer scientist; he did a summer internship at the National Security Agency when he was young. He decided it wasn't for him because it was so boring."