WHITE PAPER

Is it Influence or Manipulation?

A Case for an Internet Code of Conduct

By Cees Links, GM of Qorvo Wireless Connectivity Business Unit

Qorvo is a wireless connectivity company. Our intent is to make our world a better place by connecting more people to the internet and to each other. More recently, Qorvo also moved into connecting more things to the internet (Internet of Things), allowing us to make better decisions, faster. The proof of the progress is the increased number of applications that are becoming essential to our daily life.

We usually do not have a good memory for how life was in the past, or how inconvenient it could be from time to time. I realized this recently, when I visited the Van Gogh Museum in Amsterdam with tickets ordered over the internet for 3:30 in the afternoon. Arriving at the museum at 3:30pm, we were just able to walk right in. I was reminded that when we visited the museum 5 years ago, we had to stand in line waiting for about 3 hours.

This example seems to be about convenience. But it is about more than that. Just think about a tourist who has now another three hours to roam around the city, visiting another museum. This regained three hours creates economic value through activity elsewhere. The reality is that the internet has become the engine for economic growth, as there are surely many more examples of small improvements creating together an avalanche of economic growth.

So, a connected world is a better world, right? This question is very much on-trend, especially in light of recent security and privacy breaches. Time to really give this question a second thought.

The Online Equivalent of the Hole-in-the-Wall Gang

These days we live in the “Wild West” of the internet – from a legal perspective, the internet is almost totally unregulated. Perhaps more importantly, the effects of the internet on our society are hardly understood. It’s not just our legislators who do not understand the internet. Many (internet) engineers do not understand it either! Well, they may understand pieces of it, but only few people have a grasp on the big picture. As a society, we are learning about the effects of the internet as we go along.

Here’s one example of this ongoing learning. Netflix knows my tastes and recommends movies to me that fit my tastes. Initially I thought this was a great Netflix feature! But I began to realize that the consequence of following the recommendations was that I was becoming more entrenched in my own bubble. What I thought was an enrichment, turned into lack of variety and made me monotonous. Made me poorer, in a sense.

Value Flip

Shifting from the Netflix example to something larger, we know by now that the internet, or maybe more specifically, the social media on the internet, has a tendency to create bubbles, where like-minded people meet, interact and agree emphatically with each other. As we do that, our bubbles seem to expand, and our perceptions become our realities – they become our version of the truth. Our critical thinking skills begin to erode, even about our own ideas, because we prefer to hang out in our bubble of "like-minds." There is a continuum of this kind of behavior, of course, but the tendency is clearly there.

This is another value flip. What seemed like a good idea at the beginning, has flipped and become negative – and with a dark side that you might not immediately suspect.

Targeting Advertising

In the same way that Netflix recommends movies, social media uses their capability to "know" us, to sell advertising. It's called "targeted advertising," and there is a lot of good to be said about it. Blanket advertising is an expensive waste, like throwing big piles of advertising folders for all kind of products into every mailbox on every street in the whole city. Again, this targeted advertising seems like a positive thing. Now I only see advertisements on things I really care about – a win for both the advertiser and for myself. (How we love living in our bubbles!)

Influence vs. Manipulation

Before explaining the value flip of targeted advertising, let's explore the difference between influence and manipulation. Advertising clearly tries to influence our behavior, and we are used to that. We have even built up a certain resilience about it – probably because we know that influence is part of our daily life, and we probably influence others as much as others influence us. So far, so good.

However, there is a dark side of influence. It's called manipulation. It happens when there is an imbalance in information between the two parties, and one party exploits that imbalance to take advantage of the other party. This is nothing new, unfortunately. One example is the advertising experiments that were performed in the movie theaters of the 1950s, where very fast ad images were inserted into the movies being shown. These images, of soft drinks for example, were so short (milliseconds), that people didn't consciously notice them. Whether these experiments led to any favorable effects for the advertiser is an open question. But once the public found out, the outcry about this type of manipulation led to the outlawing of this type of "subliminal messaging" in many countries.

The Value Flip of Targeted Advertising

If social media start to know us so well that they know our weaknesses, our uncertainties, our vulnerabilities, then they can exploit that by selling this knowledge to advertisers. Targeted advertising suddenly flips to its dark side, and instead of being influenced, we are being manipulated.

Even if we have approved the third party (the advertiser) to inspect our data via our dealings with the social media outlet, did we really make an informed decision that this would lead to manipulation? But that has become the reality. The imbalance of information is exploited by "big data" and "artificial intelligence" applied to the information we reveal about ourselves by using social media, and that exposes us to become victims of manipulative advertising.

This manipulative advertising can be subtle, like phishing, or less subtle, like data theft. When the information of large groups of people is obtained, and those groups are then bombarded with very specific targeted messages, it can have huge impacts. As we now understand, it can tilt the outcomes of elections.

Is a Code of Conduct Needed?

The internet is a new frontier, and it probably is comparable with the Wild West, with no law and order yet established. Invented by great minds and put together by great engineers, certainly, but as a society, we are still in the early stage of learning about the impacts on our daily lives. And we still have a long way to go to deal with the consequences.

Cars and traffic would be a good analogy here. Simply put, a car is a tool that conveniently takes us from point A to B. At least, that's probably the way it started. Of course, today, a car is not just a simple tool. It's about driver's licenses, traffic rules, police and highway enforcement, traffic accidents, car insurance, freeways, gas stations, gas distribution, traffic congestion, traffic reports, the list goes on and on. It probably took us 50 years to establish this car ecosystem, this fabric, that we are conveniently using every day, as if it has always been there. And it's still evolving. Even today, also in Qorvo, we continue to work on improving traffic safety, and other technologies for self-driving cars. Qorvo wireless products help sense danger, connect information and protect lives. Innovation is never-ending, especially as the automotive infrastructure further evolves with smart cars and smart cities, much like the internet is evolving.

Switching back to the subject of internet security, I recently wrote an email to a friend about a particular subject, buying a car of a certain brand, and I assumed that the email was completely private. However, to my big surprise that same day, I received an advertisement on social media about that brand, and a deal especially made for me. Coincidence? Perhaps. Or perhaps not.

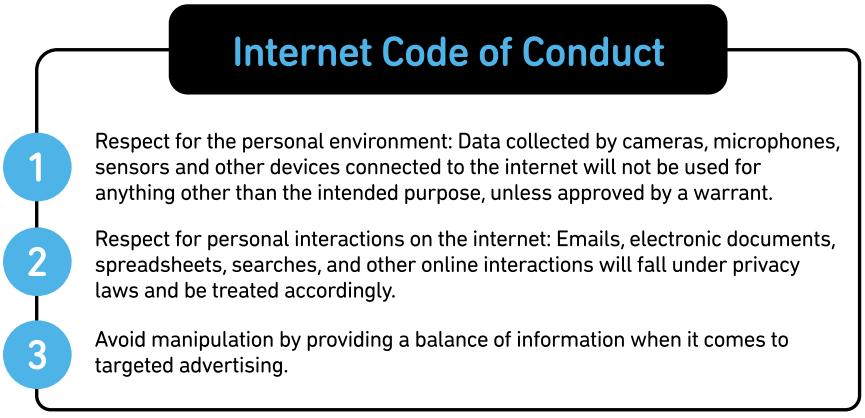
In the physical world, the privacy of correspondence has been protected for centuries. Tampering with the mail is considered a felony crime in the U.S., for example. Why is this assumption of privacy broken when we move to writing an email and sending it over the internet? Similarly, we know that in the physical world, our houses cannot be entered without a warrant. But if I bring in devices and sensors, including cameras and microphones, can I still consider my home secure? More specifically, am I really waiving all expectations of protected privacy? Can the data generated by these devices be freely used for targeted advertising? Is my voice assistant only "listening" when I call out the key word? Or can my personal situation now be exploited freely all the time?

Will it take 50+ years to make the internet a safer place? Will it take 50+ years to sort out the difference between influence and manipulation? I definitely hope not! Can we wait for legislation? Probably not. Do we need a code of conduct for the internet now? It sure seems like it.

What Would an Internet Code of Conduct Include?

Probably it's not that difficult to get started. The code of conduct for the Wild West was pretty straightforward. Basically, it was, "let's pretend we live in the civilized world and comply with the rules of the physical world as if enforcement was in place."

A code of conduct for the internet, the virtual world, should also mirror the rules of the physical world and adopt those rules without any enforcement being in place, while we wait for legislation to (maybe) catch up. Perhaps these three elements are key:



It seems to me that these rules sooner or later will be implemented in the internet, for the simple reason that they make sense. They have made sense in the physical world for hundreds of years, why would they not make sense in the virtual world?

Nothing Good Comes for Free

The internet is indeed a great invention. And it should not be dominated by a few large companies that are able to determine law and order as it suits them. We are dependent on the internet, as anyone who has tried to go a weekend without using it can attest.

We often hear a response to breaches of privacy that goes something like, “well, these online applications are all free to use – what did you expect?” It reminds me of my mother warning me to be very careful if something is offered for free, as there is nothing free in this world…. Have we been too naïve as individuals? Is that the same as knowingly waiving our privacy? Have we been too naïve as a society? Does that mean we are okay with elections being influenced? Maybe. Or maybe it is part of growing up and understanding what the intricacies and the dangers are – and learning how to protect ourselves. This may cost us some money, but maybe it’s worth it?

Recently I was asked whether self-regulation or imposed legislation of the internet would stifle innovation. My first thought was that it probably would – and fair enough, because we have some cleaning up to do! We have gone a little ahead of ourselves and assumed a little too much freedom in the Wild West of the internet without understanding the price.

But after thinking about it a while longer, I realized that making the internet a safe place and a fair environment is an innovation challenge in itself. So, in that sense, self-regulation or legislation does not stifle innovation at all. It steers the internet in the right direction. It is just an example, albeit a very important example, of market feedback for engineers and innovators to develop the right products.

At Qorvo, we believe that a connected world is a better world. But this better world does not come for free. This better world is something that we need to understand, believe in and fight to make right.

About the Author

Cees Links is a Wi-Fi pioneer. Under his responsibility, the first wireless LANs were developed, ultimately becoming household technology integrated into PCs and notebooks. He also pioneered the development of access points, home networking routers, and hotspot base stations. He was involved in the establishment of the IEEE 802.11 standardization committee and the Wi-Fi Alliance. He was also instrumental in establishing the IEEE 802.15 standardization committee to become the basis for the Zigbee® sense and control networking. Cees Links was the founder and CEO of GreenPeak Technologies, which is now part of Qorvo, and has become the General Manager of the Wireless Connectivity Business Unit. He was recognized as **Wi-Fi pioneer with the Golden Mousetrap Lifetime Achievement award**.

For more information, please visit **www.qorvo.com**.

About Qorvo

Qorvo (NASDAQ:QRVO) makes a better world possible by providing innovative RF solutions at the center of connectivity. We combine product and technology leadership, systems-level expertise and global manufacturing scale to quickly solve our customers' most complex technical challenges. Qorvo serves diverse high-growth segments of large global markets, including advanced wireless devices, wired and wireless networks and defense radar and communications. We also leverage our unique competitive strengths to advance 5G networks, cloud computing, the Internet of Things, and other emerging applications that expand the global framework interconnecting people, places and things. Visit **www.qorvo.com** to learn how we connect the world.