Power and domination as challenges of an emerging "internet of things".

Niels Gottschalk-Mazouz, University of Bayreuth (Germany)

Talk delivered at the AAP, Canberra (6.-11.7.2014), 8.7.2014, and at the Conference „Philosophy and Social Science", Prague (23.-26.5.2013), 25.5.2013

Since quite a while I am working in Philosophy of Technology as well as in Moral Philosophy and Political Theory. It seems quite obvious that there are certain kinds of challenges, political and moral, that come with certain kinds of technologies, like nuclear energy or genetic engineering. Some of these challenges can be nicely addressed via the development of political institutions or moral guidelines. Some other of these challenges, however, require a more in depth understanding of "what is going on" and "what is at stake" before eventually being able to come up with such "solutions". They require more analysis, or, in the first place, a description in terms that allow for adequately thinking about them (and about possible solutions).

To me, the current development of the internet is such a case. Since quite a while there has been a discourse accompanying its development that is expressing high hopes on the one hand (knowledge open to all, consumers become producers in the Web 2.0, social networking, facebook revolutions). These hopes are only slightly damped by what was called the Digital Divide, i.e. that only some can benefit from the internet for it needs not only content, but also access and basic skills to do so. The more dystopian scenarios come under the heading of the "surveillance society" focussing not only on the internet but on Information and Communication Technology development more broadly, including Telecommunication, Closed Circuit TV and so on. First it was the state, now it is private companies that are seen to collect as much data about the users as they can, combining it and using – or now: – selling it. While the aims of surveillance might be different ("security" vs. "profit" by creating a "better user experience"), these companies do conform to the laws of the states where they are active of course and do serve state purposes, like in the USA under the patriot act turning over data to Homeland Security for further processing.

Of course, the users anticipate all this, the camera surveillance of the public sphere, the possible surveillance of telecommunication, of internet communication, and this adds to

the intended effects of surveillance, by anticipation of ex-post sanctions, incorporation of standards and rules and formatting of thought that is. For such a constellation, the term "control society" was coined by Michel Foucault and Gilles Deleuze. In the critical discourse on ICT and the Internet, this is often seen as the worst case scenario, and possible counterstrategies are discussed.

This is a very rough sketch of the discussion, but if you have a look at the literature then you will see that this is indeed the main dystopian scenario – if we set aside science fiction scenarios like getting imprisoned in a matrix or being dominated by some autonomous supercomputer some day or the like.

Now, I think that this analysis is based on a view of ICT and the Internet that is too narrow and short-sighted. It has to be complemented by an analysis that focuses on current developments and trends in these fields if it does not want to appear out-dated or even naïve. These developments and trends that I am thinking of have been summarized under the heading of the "internet of things" or "ubiquitous computing". In this paper, I want to explore how they modify the old challenges (i.e. of the surveillance society) and what kind of genuinely new challenges they might bring. While the modifications are discussed in the literature, the genuinely new challenges go largely unnoticed, at least that is my impression from the literature, so this is where I have been trying to come up with some useful distinctions to analyse what is going on, what this might mean to us and where possible challenges lie.

So, what is this, "internet of things" and "ubiquitous computing"?

The "internet of things" means that physical objects are connected to the Internet, through technologies such as radio frequency identification (RFID), sensors and smartphones. Internet-enabled objects can share sensor data with web services and applications. As the physical and virtual worlds begin to interact with one another, boundaries between these worlds begin to erode. Our interaction with computers moves away from the desktop and into the environment, and becomes increasingly intertwined with our everyday lives. As this happens, we lose the ability to examine the artifacts we interact with as computing technology. They become invisible and infrastructural.

((This was a quote from a recent call for papers for a Special Issue of the journal Ethics and Information Technology in the Internet of Things.))

“Ubiquitous computing” sets a different accent. Here, not “dumb” things are hooked up to the internet allowing mainly for input, but maybe also for output operations, i.e. only serving as an interface (as I would say is the case in the “internet of things”), but the things become smart things, computing things, itself. Here is a quote from Mark Weiser, one of the pioneers, from 1996:

Inspired by the social scientists, philosophers, and anthropologists at PARC, we have been trying to take a radical look at what computing and networking ought to be like. We believe that people live through their practices and tacit knowledge so that the most powerful things are those that are effectively invisible in use. This is a challenge that affects all of computer science. Our preliminary approach: Activate the world. Provide hundreds of wireless computing devices per person per office (…) This has required new work in operating systems, user interfaces, networks, wireless, displays, and many other areas. We call our work "ubiquitous computing". This is different from PDA's, dynabooks, or information at your fingertips. It is invisible, everywhere computing that does not live on a personal device of any sort, but is in the woodwork everywhere.

So “ubiquitous computing” means an infrastructure that contains standardised IT elements with ad-hoc node updating, such that the virtual-real and online-offline distinctions vanish in a so-called “augmented reality” or better yet in “augmented actuality” because it shall support us in your actions, not only by providing information but by being a smarter thing that you can use more efficiently or for more purposes than before – I would say. In fact, this smart infrastructure is already about to develop, due to two trends: Computerization and networking. So, PC/tablets, smartphones, payment terminals and ATMs, cars, cameras, door locks or other ingredients of the smart home are just the most visible first instances of a “robotic infrastructure”, as I would say, that also comprises large parts of transportation, communication, water and electricity supply infrastructure, of smart (computerized and networked) things that we more and more rely on in our actions.

Before we explore the consequences of this further, let me quickly point out what the internet of things and ubiquitous computing means within the old, surveillance discourse. Surveillance gets much easier, because so many sensors are around, so many things are around that are sensed by the sensors, and because those sensors are networked. People voluntarily or involuntarily make sensor data, and other data,

available and let it flow. This is so because the internet of things makes sense only if there is widespread exchange of information. This, of course, brings enhanced surveillance possibilities "by design". Now, ubiquitous computing brings further enhancements. If you use smart things to do something, like opening a door or driving with your car, the monitoring of these actions is possible without any additional sensor data; it is possible as reporting by the smart thing itself. Again, this thing is networked and is useful only insofar it is networked, so surveillance possibilities are built-in by design.

The data, by the way, is not only about the user himself, as has been evident from uploaded picture and video that frequently (normally?) show others, from uploaded phonebooks, etc. – or if it comes to actions, in general the data is also about others insofar as our actions are interactions. One intentional use of this effect has been dubbed "sousveillance" (Steve Mann), surveillance from below, so to say, which is the recording of an activity by someone that is involved in this activity where the activity involves other individuals or corporate or state agents.

To be able to see genuinely new challenges, my suggestion is to focus on that part of the internet of things, where the things are hooked up to the internet as output, can be altered in their functioning. For ubiquitous computing, this is the very idea anyway: That our things get smart, those things that we use in our life. The main idea of this paper is to realize that these things are means to act. So the "internet of things" should not be seen merely as of things, but as things that are means to act, and to act also in domains that are crucial for the user, and that can be altered from the outside, that can be modified or disabled. This, I think, points out the main difference to the older, surveillance discourse. The moral and political worries should be not only about information, about who knows what, but about who can do what, in the sense of having suitable means at hand or not, that can be employed to realise one's aims. In the new world of smart things, those who control these things no longer have to use misinformation or threat to keep people from doing certain things (or force them to do certain things), but they can directly intervene by controlling the means of action. Earlier, they could only feed information and react on information they obtain by surveillance (if they could react), now they can block (or enforce) actions much more directly.

To explain this in more detail, I want to invoke a common model of action. If action is the aim-oriented use of means, the action cycle consisting of aiming, employing some means, evaluating the success – and then aiming again. The old discourse is about information and opinion, and this affects the aiming and the evaluation phases. So in a certain sense it is possible for third parties to control actions, by misinformation that is. But this is only an indirect control, for the actor can still do what might be unwanted that he does. Whereas in the new control discourse, the employment of means is affected and should be addressed. This goes far beyond issues of surveillance and privacy, comprising issues of basic autonomy, power and freedom (as will be explained later).

As I said, the whole idea of these "new means" is that they are connected and smart. This creates intrinsic interdependencies. E.g., to stay smart, our things need continuous updates (like your Computer or Mobile Phone is already getting, for the OS or the Antivirus is a good example), or they require that you are continuously online anyway (if you use software as a service). This gives others partial or full control over your device, and not only in an on/off fashion, but in a more complex way. I would say that we move from a world of static means (static tools) to a world of dynamic means, of means that are ever changing and that the user cannot (and does not want to) fully control in their dynamics – let alone keep them constant which would render them useless immediately or with time.

On the other hand, one can use the robotic infrastructure to produce new, static tools and objects. Like, download a public blueprint for some automatic rifle and use a 3d-printer to build such a rifle at home (as it happened in the US). You could also build "discursive things", i.e. tools that counter surveillance measures, etc. – I do not want to discuss this further, because this then just leads to the question of who controls the blueprints or the printers (that are dynamic means).

I just want to point out that one can make the difference between the old, information-and-surveillance-centered discourse and the proposed new, action-and-control-centered discourse also in terms of knowing-that and knowing-how. The standard internet view is that it is all about knowing-that, explicit knowledge (or better knowledge candidates), in form of texts, pictures, sound (wikipedia, youtube and so on) etc. Also surveillance is all about knowing that this and this is the case or not. In the

control-centered discourse, the internet is seen as about knowing-how, i.e. implicit knowledge that enables somebody to do something. And this is not in the form of recipes for cooking, but until now in the form of programs/apps that you can download. So, concerning your personal computer or the things you can do with it, the internet has always been providing knowing-how. Now, this is no longer confined to your personal computer. You can download firmware, apps, training data, blueprints etc. for all these smart things that you use as means to act. And you can upload them as well. What we see so far might only be the beginning. So the "new" internet of (smart) things is also about knowing-how. And so is the control-centered discourse.

With regards to the surveillance discourse, I think one can argue that the evolution from surveillance towards controlling the means is only natural. Automatic surveillance as we have it today already renders huge amounts of data that can be evaluated en masse only automatically. But then one wants to react on the results of surveillance. Any good surveillance society would this want to happen automatically. Because, if the aim is to supress certain actions, then a very efficient way is of course the manipulation of the means to these actions. This way it could happen large-scale, immediately, stealth and without large – and maybe unreliable – personnel.

To be able to better express what is at stake I would like to introduce now some vocabulary of practical philosophy, that of power, control and domination.

1. "Having power", or "be powerful", I want to say is "being able to 'do' something", "being able to make something happen" or "being able to act".

2. To control an object x is to have power over x, which is "being able to make something happen (or suppress something from happening) on or with x.

3. To control a person P is to have power over P either like an object, or by controlling his actions, i.e. make them happen or prevent them from happening, by influencing P's aims or means.

4. To dominate a person P is to control P according to the dominator's interests only.

To control an object, I would say, is morally neutral. To control a person is problematic (because autonomy is at stake; but maybe we do so for paternalistic reasons…). Finally, to dominate a person is morally wrong.

So, by controlling an object x that some person P uses as a means, we are controlling this person as well, and we may be dominating him if we are controlling according to our interests only. This control may be only partial if there are alternative means available. In any case, we are interfering with his ability to act. And this is a question of power, of who has the power so to say. And with certain powers, like those to move or to perform certain actions, also our freedom.

According to this, I would say that the full-blown dystopia is monopolistic – or, as things are – oligopolistic domination, by control not only of information, but by control of our actions according to the interests of others. And insofar as these others are acting as instances of systems, like the government or the economy, that strive to dominate and control the lifeworld in which we act, it is only fair to call this dystopia the colonialisation of agency.[1]

Now, these dystopias might seem a little dark. I do not think that we are clearly or inevitably moving towards a full-fledged surveillance society or control society. But I think that is only realistic to acknowledge that some state and private agencies have access to our data, unofficially or officially, and that at least occasionally also criminals and others get access to them. So there is surveillance going on to some degree. And I think that we should understand what it would mean if we get not only under surveillance to some degree, but under control to some degree, in the sense that we are no longer the masters of our means to act.

[1] I am indebted to Matthias Kettner for suggesting this critical-theory term in the discussion of my talk in Prague.