HAL open science

# Diagonal mass surveillance: Gulliver versus the Lilliputians

Didier Bigo

▶ To cite this version:

Didier Bigo. Diagonal mass surveillance: Gulliver versus the Lilliputians. 2014. hal-03393004

HAL Id: hal-03393004

https://sciencespo.hal.science/hal-03393004

Submitted on 21 Oct 2021

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution - NonCommercial - ShareAlike 4.0 International License

# Diagonal mass surveillance: Gulliver versus the Lilliputians

opendemocracy.net/can-europe-make-it/didier-bigo/diagonal-mass-surveillance-gulliver-versus-lilliputians

Didier Bigo

Mass surveillance does not follow the vertical logic of pure state surveillance as imagined by Orwell. Rather, it is diagonal – building on the information we voluntarily disclose to engage in our own "surveillance" of online friends. This makes it much more perverse.

Filipino protesters join global protest against mass surveillance, February 2014/Demotix/Ezra Acayan/All rights reserved

In the wake of disclosures by Edward Snowden about the NSA practices concerning PRISM and other US surveillance programmes like Xkeyscore, Upstream, Quantuminsert, Bullrun, Dishfire, and the close involvement in these activities of services like the GCHQ (Tempora program), there is an urgent need for a systematic assessment of the scale, reach and character of contemporary surveillance practices, as well as of the justifications they attract and the controversies they provoke.

The public needs to know whether these practices mark a significant reconfiguration of, say, relations between intelligence gathering and surveillance of the Internet and other systems of telecommunications, or mark sustained challenges to fundamental rights in the digital sphere.

There is also a need to pay close attention to the longer-term implications of practices that have already raised serious questions about the widespread transgression of legal principles and democratic norms. And finally, to how transnational surveillance resonates with contemporary shifts in the locus and character of sovereign authority and political legitimacy.

Revelations about practices of large scale surveillance that branch out into the surveillance of everyday activities and bulk intelligence gathering on big groups of people has rightly generated considerable controversy. Yet, there is a danger that both the popular and scholarly debates will be reduced to familiar narratives about technological developments reshaping relations between the watcher and the watched, or the fulfilment of predictions by Georges Orwell or Philip K. Dick, or the transformation of

representative democracies into totalitarian regimes in the name of protection.

No – what we see here is not a horizontal system of surveillance (a rhizome), where surveillance is pervasive but not centralised, and in which we participate because we individually want to take advantage of surveillance (for example by seeing what our friends do on Facebook), or that we enact through voluntary disclosure of information to online friends. Nor does this system follow the vertical logic of pure state surveillance imagined by Orwell in his novel *1984* (a total surveillance).

## The diagonal of the bishop: surveillance and intelligence in a transnational world

The current situation could be best conceptualised as a tri-dimensional chess bishop, a "diagonalised" form of surveillance and intelligence. The meaning of the acronym PRISM is revealing in this regard: Planning Tool for Resource Integration, Synchronisation and Management. This long range, diagonalised form transforms the horizontal network of everyday surveillance (e.g. our individual and voluntary use of social media) into the vertical emergence of relevant information.

This selection from bulk of what information is relevant and needs to be investigated is an automated process, regulated by complex algorithms and the use of specific keywords. There is thus a double movement, from the inside out and the outside in, where personal information is voluntarily shared but then secretly recaptured by intelligence agencies. The watched, therefore, participate in their own surveillance.

The fact that these practices ignore national borders and treat information in bulk raises a series of questions. Of these, two are central. The first one concerns the conceptual disconnect between the idea of an interstate world in which each state has a clear vision of its own national security and the practices brought forward by global surveillance. Current surveillance practices involve a network of different intelligence services (the so-called Five Eyes plus) sharing some information in the name of global antiterrorism while also acting against their partners in the pursuit of their own national security interests, thereby destabilising traditional understandings of alliances and state behaviour.

The second consequence concerns the strategies deployed by multiple actors to resist surveillance practices, through diplomatic or legal means, as well as adjustments in everyday online behaviour by Internet users. A crucial question is thereby posed: will these users continue to participate in their own surveillance through self-exposure, or will they develop new forms of subjectivity that give more thought to the consequences of their own actions?

Intelligence work begins as analysts use the data collected through large scale surveillance with the goal of identifying unknown persons related to a targeted individual or group, within three degrees of separation ("hops"). For example, if a suspected individual has 100 Facebook friends, the person in charge of the surveillance at the NSA or one of its private subcontractors can without warrant follow the communications of friends of friends of friends, for up to three hops – about 2,669,556 people.

Faced by the magnitude of data accumulated, the strategy used by the analysts is not to read all the content of these communications, but to visualise the graph of interpersonal relations ("meta-data") hoping to disconnect specific connection nodes. This is far from a full reading of everything the data contains, but also equally far from a scientific method that would give a required level of certainty and any semblance of truth to the results.

This method is essentially suspicion elevated to the rank of art. It depends on the analyst's intuition and interpretation, and the results may be contradictory from one analyst to the other. The fear of an omniscient big brother is mostly irrelevant in this scenario, as the claim of any truth coming from this visualisation must be a false one, based as it is upon the pretence that predictions can be elaborated regarding specific human actions at some point in the future, when even general forecasts about trends are difficult. Technology is used as if it could provide scientific certainty about the future, but this belief

in the power of 'big data' has more to do with blind faith than with any kind of certainty.

Artist Kaya Mar portrays Barack Obama spying on a blindfolded USA, July 2013/Demotix/Pete Riches/All rights reserved.

## National security and the digitisation of the *raison d'etat*

These ways to gather and share information have paradoxical effects on national security requirements. Namely, national security is not national any more: different national security imperatives may clash between allies and trust is eroded. The digitisation of national security creates big data gathered at a transnational scale, blurring the lines of what is national as well as the boundaries between law enforcement and intelligence.

These methods encourage a move from the judicial framework of criminal police to preventive, pre-emptive, predictive approaches, and from a high degree of certainty about a small amount of data to a high degree of uncertainty about a large amount of data. The hybridisation of public agencies and private contractors destabilises the process of socialisation via national state interests and thus secrecy, opening up the potential for major leaks by persons holding incompatible values (as in Snowden's case).

To say this more theoretically, the change and uncertainty surrounding the categories of “foreign” and “domestic” is dispersing them through the webs of multiple interconnections. This transforms the line that clearly separated the foreign and the domestic into a Möbius strip. By projecting national security inside out, via a transnational, public-private alliance of national security and sensitive data professionals, an unexpected outside comes into effect whereby every Internet user is targeted. These “data subjects” must react in turn, if they do not accept a situation where nearly all internet users are treated as potential suspects and on principle, not innocent.

## Multiple sites of resistance

In this regard, the Snowden revelations set off a snowball effect of distrust among the actors who initially thought that they were gaining from exchanging data with the NSA. The recent partners of the Five Eyes plus (Sweden, Germany, France) felt betrayed when the NSA and GCHQ publicly defended their actions by asking something along the lines of, "You knew that we were spying on you all and your heads of state. Were you so naïve as not to have imagined what we were doing ?".

The same argument has been used to confront the broader public and internet actors, some of whom (such as Google, Yahoo or Facebook) denied all knowledge of the extent of these surveillance practices. The NSA and GCHQ argued that their practices were not the problem, but rather our collective naivety in trusting them, when obviously we did not have to.

This trick may save them from juridical claims by forcing courts to consider that internet users did not have a reasonable expectation of privacy when they sent their emails. Yet, by indirectly acknowledging that they are not to be trusted, they have destabilised their own system of legitimisation. For example, the Snowden revelations have pushed private telecom providers such as the French company Orange into inspecting their technical infrastructures (notably the submarine cables that link Europe to North Africa or Asia), in order to discover that the NSA had abused their initial, more legitimately motivated collaboration (fighting against terrorism and organised crime) by secretly installing backdoors to intercept communications going through the main nodes in France, Germany, Sweden, the Netherlands and possibly Brazil.

The politicians of the Five Eyes plus countries are now caught between their official support for fighting terrorism by all means, Americanophilia, the arguments for a common alliance, and the aggressive behaviour of the Five Eyes network. If most of them consider that they have succeeded in silencing resentment from within the state apparatus (investigative magistrates or prosecutors for example, who are theoretically the 'end users' of gathered intelligence), they have not so far managed to do the same with the private providers and even less with civil society.

Hundreds of judicial claims coming from very different groups – internet actors, telecom providers, NGOs, political parties and citizen movements - have been launched with very different motives in each case, and it will be impossible to accommodate them without engaging in profound reform. The NSA - a Gulliver who wanted to know everything about everyone - has just managed to mobilise all the Lilliputians and might soon be paralysed by their minuscule but solid nets.

*This short intervention is part of a longer collective article co-written by Zygmunt Bauman, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, Rob Walker.*

***Read more from our 'Joining the dots on state surveillance' series here.***

---

[1] Barack Obama, following one of the 45 recommendations of the review group on intelligence and communication technology delivered on 12 Dec 2013, seems ready to restrict the search without warrant to two "hops" (i.e. 16,340 people), while keeping the principle alive.