Corporate transparency is crucial, but it must also become far more meaningful
De Hert, Paul; Kloza, Dariusz

Published in:
The Privacy Surgeon

Publication date:
2014

License:
Other

Citation for published version (APA):
De Hert, P., & Kloza, D. (2014). Corporate transparency is crucial, but it must also become far more meaningful. The Privacy Surgeon.
Corporate transparency is crucial, but it must also become far more meaningful

Last week – to a surprisingly muted public reception – Apple became the latest addition to a growing club of companies that have adopted greater transparency in their dealings with government agencies. In this article Paul De Hert (VuB-LSTS & UvT-TILT) and Dariusz Kloza (VuB-LSTS) outline the growing trend to transparency and argue why such information must move from being merely “available” to being “meaningful”.

Who, what and why?

Since the beginning of the decade, more and more companies, especially Silicon Valley giants, voluntarily issue
transparency reports on a regular basis: Google, Apple, Dropbox, Facebook, Microsoft (comprising also Skype) and Twitter, to name a few. (They do this voluntarily in a sense they are not forced by a state to do so. Some do it because they are pushed by advocacy groups.) These reports are freely available on-line, often in various languages, with access to archived reports, and are accompanied with an explanatory note in a plain language. They usually form a part of a bigger “package” containing also a policy on dealing with requests for disclosure or removal, guidelines for law enforcement and other relevant stakeholders, and – finally – some commentaries, blogs and/or FAQs. In addition, recently some of major international players undertook certain policy initiatives aiming to revisit surveillance practices, such as the Digital Due Process, Reform Government Surveillance or Coalition Against Unlawful Surveillance Exports. The oldest transparency reports to our knowledge were those published by Google (2010) and Twitter (2012).

Transparency reports are beneficial for at least four reasons: democratic control, human rights compliance, corporate responsibility and a potential for forcing change.

These reports usually contain two categories of statistical data. The first consists of disclosure and/or content removal requests by right holders (or entities acting on their behalf) about related copyright infringements. The second category relates to requests by governments, usually if a matter at stake is of state security importance or deals with combating or investigating a crime. As privacy lawyers, the latter provides us with more food for thought.

We think transparency reports are beneficial for at least four reasons: democratic control, human rights compliance, corporate responsibility and a potential for forcing change. From the viewpoint of democracy, by publishing the figures on information or removal requests, they allow these societies to control the execution of powers vested in their governments, especially those of state security and criminal policy. They give a picture, though incomplete, of government surveillance and allow to double check on the data governments themselves are willing to give us about their surveillance practices. As Google puts it, “We publish this information to shine a light on how government actions can affect our users and the free flow of information online”.

From a human rights viewpoint, by their own policies and practices on disclosure, these reports demonstrate how companies respect certain fundamental rights, such as the right to privacy. We learn from these reports that requests are not treated automatically, not all of them are complied with, and personal data of individuals concerned can be kept confidential. To illustrate this point, in the first half of 2013 Microsoft “disclosed content in response to 2.2% of the total number of law enforcement requests received” and Twitter states “We may seek to narrow requests that are overly broad”.

Note that not only privacy is served by a restrictive attitude towards disclosure demands. Corporations, by doing it, also serve the freedom of expression and the freedom of news gathering: the European Court of Human Rights, for example, acknowledged in Youth Initiative for Human Rights v. Serbia (2013) that “the refusal of the intelligence agency to provide … with information as to the use of electronic surveillance measures had adversely affected … [the] ability to exercise … [the] role as a public watchdog”.

From the corporate responsibility viewpoint, these reports show how seriously companies take some societal values, such as privacy, and how trustworthy such a company is. This can give them competitive advantage above those that treat these values less seriously. (Obviously, it is also a public relations tool.) On top of that, as this refers more to governments than to companies, from the governance viewpoint, their value lies in their educative and persuasive nature that might lead to a desirable change, e.g. by “naming and faming” or “naming and shaming”. Put simply, monitoring is one of the enforcement mechanisms, often practiced in the human rights area.

At the end of the day, a transparency report is not the goal in itself, it is a means to achieve a socially acceptable execution of government powers.
Corporate transparency is crucial, but it must also become far more meaningful » The Privacy Surgeon

Transparency reports, however, tell us very little about trust

But all it is not as good as it looks. Some half a year ago, Ryan Budish pointed out that “transparency reports actually tell us very little about whether we should trust … companies”. A mere analysis of the figures only gives an impression about “the aggressiveness of law enforcement and intelligence agencies”. We can see that company A got, in the last reporting period, X requests and complied with, say, Z per cent of them, but the company B got only Y, complying with, say, twice as much. And in comparison with previous years, it doubled, or event worse, tripled. (New problems with evaluations might arise as some companies can receive fewer requests. Why? The contents from open platforms, such a Twitter, usually do not “need a warrant … only a web browser”.)

Also, reading these transparency reports leaves a lot of important questions unanswered: What actions did these companies take to protect our personal data, and – broader – human rights in general? Did any of them ever question any of the requests? As their experience grows, do they pressure governments for a change? Do they fix their own disclosure policies and practices? “It would be wrong to mistake transparency reports as any indication of corporate trustworthiness,” concludes Budish.

Environmental protection holds a useful example

Public reporting is not a new tool of governance per se. For example, it is well known in the field of environmental protection. What can its experience teach us?

American companies report annually the quantity of hazardous chemicals that they have released into the environment or transferred off-site. The US Environmental Protection Agency then incorporates this information into the Toxic Release Inventory (TRI), which is a nationalised public on-line database, and subsequently issues an annual report naming those facilities that have released the most toxic substances. (For a European example, see e.g. Risicokaart van Limburg.) Such reporting often brings two main benefits. It forces change in the behaviour of the companies (“I don’t want to be named the worst polluter”) and allows individuals to make informed decision (“I don’t want to live near a very hazardous facility”). One could argue that people can access such data by means of the freedom of information request, but it is the TRI that had shortcut the bureaucratic information request and made these data truly accessible.

In order to truly achieve their goals – democratic control, human rights compliance, corporate responsibility and a potential for a change – transparency reports must be truly meaningful. That is to say, these reports must be comprehensive, verifiable and understandable.

Opponents of measures such as TRI usually argue that data gathered are sometimes difficult to understand and fully exploit, that these data might be misrepresentative without context (both reasons due to lack of technical knowledge impeding interpretation) and that chemical volumes are alone poor indicators of human health risks. Individuals, overwhelmed by the amount of information, if not affected directly by an environmental hazard, are unlike to pay attention to the data so “remote” from them. Finally, to avoid reporting, many companies switch to use the chemicals that they do not need to report or simply fail to report. Thus, commentators often agree that “in a first place the data should be clear, put into context and cover as many facilities as possible.”

Transparency reports are good, but more is needed

In the quest for an optimal policy on transparency reporting, the current practice thereof (i.e. they tell us very little about corporate responsibility and trust) and the experience of its environmental counterpart holds some useful lessons. In order to truly achieve their goals – democratic control, human rights compliance, corporate responsibility and a potential for a change – transparency reports must be truly meaningful. That is to say, these
Corporate transparency is crucial, but it must also become far more meaningful » The Privacy Surgeon

reports must be comprehensive, verifiable and understandable. Nowadays they have become plausible developments, but still more is needed.

Why comprehensive? As of today, we have a (relatively small) number of global players disclosing their statistics about various countries that have requested somebody’s data in a reporting period. Sometimes some “local” players provide their data too. Yet statistics from telecoms are disclosed under a separate regime. But we believe that until all players do so and that they will cover all governments’ attempts to get data, we will never get a complete picture. (Recently, the Art 29 Working Party, a EU advisory body for data protection matters, called for “some form of general reporting on surveillance activities” to be put in place.)

Why verifiable? By merely a voluntarily disclosure of statistical data, we are supposed to trust in companies’ good will and in their due diligence while calculating these digits. However, we should “trust, but verify”. Until governments themselves publish similar data and until journalists, geeky individuals and/or NGOs start making analyses, aggregations and comparisons – in other words: auditing – we will never know if both parties say the truth. (It is factual that some governments or government’s control agencies publish such statistics, but they are far from comprehensive, thus making the verification incomplete; examples include Poland, about telecoms data retention and Hong Kong, about Google.)

Why understandable? Merely showing statistical data that a government X or Y asked Z times about someone’s data is a good first step, but more is needed: not only information, but also knowledge. Until transparency reports are explained fully and clearly, we will never grasp the scale of surveillance practices. In particular, we need clarification on:

- what categories of information have been sought (identity, IP address, activities on-line, etc.),
- for what purposes (state security, crime prevention or investigation or – simply – a divorce),
- by whom (security agency, public prosecutor, court, etc.),
- how our personal data are protected (what these companies can do and what they actually do), and
- what implications for the individuals and for the society these disclosures have.

(Yet we note that some transparency reports give some of these data; a good second step.)

Meaningful transparency reports

Transparency reports recently became a standard in the practice of ICT companies and it can be expected that these companies will continue their publication. In the contemporary world, in which governments and other relevant players are more and more interested in our private lives and turn to all kind of sources, including private ones, these reports help us to understand what happens with our personal data. In this short post, however, we have pointed out a few modest suggestions for the direction of transparency reports’ expansion: comprehensiveness, verifiability (double-checking) and understandability. This would make these reports more meaningful, turning them into a valuable tool of privacy governance.

We thank Jamal Shahin for his useful suggestions. Section about environmental reporting comes from Dariusz’s speech at KnowRight 2012.

Related Posts:
May 15, 2014

Corporate transparency is crucial, but it must also become far more meaningful » The Privacy Surgeon

Now Microsoft has raised the bar
US wiretap case could be the key to
Beware the NSA’s contrition tactic
Weekend reflection: All

The PrivacySurgeon is owned and operated by Simon Davies - Initial design by Scarab Designs Ltd - Implementation, coding and maintenance by Jim & Pete.

> Privacy policy