Interview Privacy Commission

For more information about this interview, please contact Mr. Maxim Chantillon (KU Leuven Public Governance Institute – maxim.chantillon@kuleuven.be)

Introductive remarks from the Privacy Commission

Do we include the private sector? The Privacy Commission (PC) asked this question because the use of geo localisation by telecom operators (Proximus, etc…) is regulated by Article 122 of the Law of 13 June 2005 on the electronic communications.

This is also relevant because, in some cases, the administrations create a partnership with the Telecom operators to offer an e-service. This raises the question of whether Art 122 should be applied then. The IBPT (Institut Belge des services postaux et des télécoms), which is the control authority of the Telecom operators, said that this was an unclear situation but that, in any case, the citizens are not well informed about the source of the service. There is often only a general clause about the "profiling" in the general terms and conditions but this is not sufficiently precise. This could be a breach of the obligation of transparency contained in the Law of 13 June 2005, as there might be more to it than the simple general interest.

Finally, the PC underlined that one of the difficulties with this law is that it doesn't apply to the "Over The Top" players (OTT) such as Whatsapp, Facebook Messenger, Skype,…

Interaction between the Federal – Regional Commissions

In order to process Federal personal datasets (such as cadastre), an authorisation must be asked to the Federal PC.

For the Regional and Communautary datasets, there is a specific supervision Commission at the Regional level (Vlaams Toezichtscommisie, Commission Bruxelloise de contrôle, no Commission yet in Wallonia).

For mixed datasets (Fed + Reg), the control is done in cooperation between the relevant Commissions. Up to now this cooperation has gone well without any major issues. This could be explained by the fact that half of the Vlaams Toezichtscommisie is composed of former members of the PC.

Final note: It will have to be seen if the "General Data Protection Regulation" (GDPR) could have an impact on this good cooperation as it states that there can only be one "Data Protection Authority" (DPA). From a legal point of view, the PC is, for the moment, the only DPA and the other Commissions are a step lower, even if it is sometimes touchy to present it like that. However, the Vlaamse Toezichtscommisie has clearly expressed its will to be considered as a real DPA. So the future situation is quite unclear.

Good understanding by the public authorities of what personal data is exactly?

Not really. The example of the licence plates was given. Many think that it is not personal data. There are a large set of personal data that is not qualified as such but rather as "technical data".

In practice, there is a big difference in understanding what personal data is, between the administrations that have an internal privacy department and those who don't.

The PC hopes that this will change with the application, as of May 2018, of the GDPR which obliges every administration to have a "Data Protection Officer" (DPO) but the PC remains suspicious about this.

Specific risks for privacy deriving from the sharing of location based data by the public authorities?

One of the major problems is that "location based data" is not considered as "sensitive data" in the Belgian legislation and in the GDPR. This is problematic because, in practice, location based data could have a big impact on the citizens but it does not benefit from the extra protection granted to "sensitive data" (such as medical data, sexual and religious orientation, …).

The PC has also mentioned that the "Advices" they drafted about the sharing of information in the public sector in general (service integrators, etc..) could be relevant for our project.

According to Article 3, §3, al.2 of the Federal Law of 4 May 2016 on the re-use of public sector information, "*the communication by a public authority of personal data for the purpose of their re-use requires the prior authorisation from the Privacy Commission*". Has the Privacy Commission already received such kind of requests for authorisation, and is any of those related to location based data?

This "Open data comity" does not exist yet. So, for the moment, the requests go through the "federal authority comity" of the PC.

It should also be noted that the Federal government has indicated that it wanted to rationalise the various sectoral comities within the PC so it remains to be seen how this will be organised in practice.

So the PC has a lot less experience with open data and anonymization, which are quite "new issues".

In practice, the Open Data Directive says that the data protection legislations have to be respected to the extent necessary.

On this basis, when public authorities publish statistical analysis, they consider that 20 variables are a high enough "granularity" that respects the data protection legislations. However, according to the PC, this is sometimes insufficient as in some cases, it is possible to re-identify the individual and thus this becomes personal data (the PC has previously had this kind of problems with the FOD Economy who wanted to publish statistics).

According to the PC, there is a great need to find a balance between data protection and Open data.

Do the public authorities, willing to allow the re-use of their public sector information, pay enough attention to whether or not the purpose for which the re-user intends to use the personal data is compatible with the original purpose of the personal data collection?

According to the PC, the FODs are aware of this at the central level but, in practice, when decisions to share data are taken at the local level, this is sometimes overlooked.

How often do the public authorities use the mechanisms of anonymization in order to allow the re-use of personal data? Do you think that the anonymization techniques used are sufficiently efficient to ensure that it is not possible to "reverse-engineer" the process in order to discover the identity of the anonymised individuals?

The big issue is to see how deep the data goes (granularity). Does it go all the way down to the person?

The PC believes that there is a real problem of anonymization.

On the issue of Big data and the risk that everything could become "personal data" through data reconciliation, the PC advises to conduct "small cell tests" to find a balance.

The public authorities should conduct this test because, quite often, the public authorities talk about "anonymised data", but this hasn't been tested and this raises issues of whether the granularity was high enough to avoid re-identification. These tests are not sufficiently done and this leads to problems.

Yet, the Belgian privacy legislation indicates that anonymization = "no possibility of decoding" = no possibility to reverse engineer and re-identify the person.

So when data has been coded but can be decoded, this should be considered as "coded data" and not as "anonymised data". This distinction is important because the rules on the processing of "coded data" is stricter than the rules on the processing of "anonymised data". The public authorities are thus tempted to qualify "coded data" as "anonymised data" in order to benefit from less strict rules.

The PC is however aware of the fact that it is sometimes hard for the public authorities to evaluate whether the data is sufficiently anonymised. It has, for example, given an "Advice" on this issue (n° 43/2015[1]) regarding the necessity to find a balance.

Another linked debate is: who should worry about this risk of re-identification? The administration or the re-user? According to the PC, a certain form of *Bonus Pater Familias* ("reasonable father") liability

[1] https://www.privacycommission.be/sites/privacycommission/files/documents/avis_43_2015.pdf (FR)
https://www.privacycommission.be/sites/privacycommission/files/documents/advies_43_2015.pdf (NL)

should apply to the authority and they should involve statisticians in the evaluation of the potential risk of re-identification of the individual before sharing their "anonymised data".
The PC gave an example of bad practice: The BCE/KBO had an agreement with the private company Graydon to share personal data contained in their database. The BCE/KBO had indicated in the licence that is was not liable in case of breach of privacy. This is extremely problematic according to the PC as the BCE/KBO than feels that this clause allows them to massively share personal data.
The PC however sees hope in the GDPR, as it contains an obligation for the public authorities to conduct an impact analysis on the possible breach of privacy of the individuals and that this should be conducted before sharing the data. So this could be beneficial if the administrations do conduct a *Bonus Pater Familias* analysis, for example by including a statistician in the analysis. The PC however fears that the administrations will only do the strict minimum in this impact analysis.
Finally, the PC pointed out that one of the major problems with anonymization is that there is too little information and education about good concrete anonymization techniques (such as "small cell tests" which are a good tool to evaluate the sufficient granularity of one's statistical data).

Most of the public authorities use standardized licences in order to allow the re-use of public sector information. Do these public authorities contact you in order to have your input on the data protection aspects of these licences?
No, never.
The central FODs (headquarters in Brussels) however have the reflex to contact the PC when they have personal data questions, but this reflex is not shared by the decentralised administrations (ex. the local branch of the FOD finance for VAT in a commune).

The GDPR will be applicable as of May 2018. This will require Belgium to refit its data protection legislations before that date. Are you aware of what is currently being done in this regard?
Some adaptations will be necessary. For example, the DPO will have to be protected by a specific status (which does not exist yet) and the PC will have a greater sanction power as it will now be able to fine the public authorities and companies who breach the privacy legislation[2].
Regarding the concrete measures that will be taken, the PC will only act as an adviser.
The initiative of the refit will be taken by the FOD Justice and the Secretary of State for Privacy and the PC will be there to answer their questions.
The PC might be called upon to formulate draft legal provisions (this kind of requests already occurred in the past but this is quite rare), but generally they only give advices on the draft law. So they intervene at a later stage. In practice, this often occurs when the Conseil d'Etat/Raad van Staat underlines that the draft law causes issues regarding Article 22 of the Constitution (Right to Privacy) as it could have a serious impact in the citizens' privacy.
N.b: the legislator doesn't even have to ask the PC's advice. With the GDPR, they will have to ask this advice but they will not be binding.
Final note: The GDPR gives more competences to the GDPR, but their budget goes down a little more every year. So, like practically all the other administrations, they will have to do more with less.

Is there an overuse of the concept of privacy (i.e. is this concept always used in a correct way – challenge: often the idea of breaking the privacy is used to avoid change or innovation)?
Yes, sometimes they use "Privacy" as an excuse when, in reality, they simply don't have the technical means to give the data but don't want to say it.
In those cases, the potential re-user then contacts the PC to ask them if this is a true problem and the PC, as an independent actor, indicates that there is actually no privacy issue.

[2] http://www.presscenter.org/fr/pressrelease/20160513/reforme-de-la-commission-pour-la-protection-de-la-vie-privee