Why Geospatial Needs to Listen to GDPR

When it comes to the European Union's General Data Protection Regulation, a suitable analogy to think about is a courtroom-based TV show. Every few episodes, the judge will 'throw out' a case because a lawyer did not collect evidence using legal means. The key thing to remember for geospatialists who watch these types of shows is that under GDPR, the incorrect collection and use of information will soon be considered as a punishable offense in itself.

The GDPR regulation, which comes into force from May 2018, is an effort to uphold privacy and anonymity rights of all European Union citizens regarding their personal information. It does so by expanding the scope and definition of 'personal data' for the digital age and it governs the business practices on how companies collect, manage and use the personal data of their European customers. In the age of social media sharing, open and volunteered geographic data, GDPR reflects an effort by government to reign in organisations who often know as much, if not more, about these citizens than the governments themselves do.

Although GDPR is often more associated with sectors which collect a large amount of information on individual customers, such as banking, insurance, and health, it is, in fact, very relevant to the geospatial industry. To think otherwise, could be a very big mistake. Consider it this way. The purpose of GDPR is to regulate the use of multiple data formats which help to identify, either directly or indirectly, any person. Direct identifiers, it should be noted, are the data types which can be easily referenced and associated with an individual (including descriptors such as a name, an ID number or username, an exact location, or a detailed description of a person's physical attributes).

What GDPR does, therefore, is force data custodians to recognise the less obvious (indirect) information types (including locational data) which can be 'linked' to an individual. Consider the following scenario. A description such as a 'brown-haired female' is of little relevance to anyone, including GDPR regulators. A description such as a 'brown-haired female who visited a certain shop', although still quite broad, narrows things down significantly. If say a marketer were to aggregate this basic description with indirect identifier information such as the approximate time of visit, waypoints on the subject's chosen transport route, CCTV footage of the individual or spending details, then the anonymity of this 'brown-haired female' is placed at risk. When thinking about information in this regard, GDPR highlights the fact that an individual's private life today depends on the standard to which third parties manage, guard and anonymise both locational data and non-data.

In abiding by these new legal mechanisms, it helps that geospatialists already understand the locational component of information (some 80% of all information) and that this information needs to be managed correctly. At the same time, however, geospatialists will need to re-examine this data and decide how to prevent it from being linked with other spatial and non-spatial datasets including transport, administrative, demographic categories. The processes and lifecycles around data collection and management will also need to be examined carefully. This includes the design of online forms, the authorisation of GPS tracking on mobile apps and the use of geolocated social media content. Custodians will need to generalise or filter identifiable features or patterns from geospatial information. A jogging app, for example, will need to ensure that it doesn't capture and store potentially revealing details on user's private activities (such as visits to political or religious institutions) while a provider of aerial imagery will need to filter out or obscure identifiable features on, say, someone's home. And just in case there is any motivation required, the custodians of such data will, from next May onwards, be liable for fines of either 4% of annual profits or 20 million euros for any non-compliance breach.

Compliance with GDPR is, therefore, as you may expect, not going to be an easy task. Organisations which need to comply with the regulation may, after all, currently be using legacy IT systems and/or outdated processes. More worryingly, in many cases, organisations will not even be aware of the types of data which they have in their possession. The requirements of GDPR are, one could say contradicted by the fact that organisations at the same time need to improve their data-sharing and interoperability capabilities in order to stay competitive. This, combined with the lack of in-house GDPR experts in data management departments, could make things very complicated indeed.

Nevertheless, where there is a headache there is an opportunity. The first step will be to recognise that data is both a valuable and potentially dangerous substance which needs to be controlled, if not defused. In order to do so, organisations will need to consider a range of legal, data management and technological approaches to protect European citizens anonymity. This will include the tricky process of implementing privacy by default and privacy by design in applications, of safeguarding information using machine-learning; of

implementing cyber-security and encryption technologies, and of explaining legal aspects of consent and permission-setting to customers in an understandable manner. Throughout this process, it is very likely that powerful geoprocessing, spatial analysis and other geo-intelligence tools (such as geofencing) will be used to meet the emerging challenges of ‘geo-privacy’.

Although GDPR is a big challenge, it presents the geospatial community with an opportunity to reinvent itself and to build better relationships with, and products for, customers. By designing transparent and flexible data management processes and by better understanding the digital footprint of data subjects, companies will be less likely to cross a ‘familiarity’ threshold which could potentially damage trust, reputation, and bottom lines. If not, just as in the aforementioned TV shows, justice will be served.

This article was published in GIS Professional December 2017

https://www.gim-international.com/content/article/why-geospatial-needs-to-listen-to-gdpr