Departing from the reliance on lengthy legalese

The use of privacy policies has become the norm for companies to comply with the EU data protection requirement to inform individuals about data processing activities. However, they have become lengthy legal documents that the everyday consumer does not understand. Cedric Burton, Senior Associate at Wilson Sonsini Goodrich & Rosati[1], questions whether there is an overemphasis on notice requirements, and analyses potential alternatives.

Introduction

The use of privacy policies has become standard practice and is certainly beneficial; they can be found offline on data collection forms, online on websites or on mobile devices and apps, and they describe a company's data processing activities. However, regulators and individuals generally complain about the lack of transparency of companies' data processing activities. In response, stakeholders tend to increase the length and detail of privacy policies, turning them into complex, sizeable documents. The question is whether this approach actually protects individuals' privacy.

Emphasis on notice requirements

EU data protection law requires data controllers to provide individuals with specific information related to their processing activities, including: the identity of the controller and its representative, if any; the purposes of the processing; the data recipients or categories of recipients; and the existence of the rights of access and rectification[2]. The obligation to provide notice is also enshrined into the requirements applicable to consent and, in particular, in the obligation that consent must be informed[3]. The rationale is that individuals must be provided with appropriate information about a company's processing activities in order to be able to provide meaningful consent to the processing and thus make an informed decision about the use of their personal data.

Looking at the letter of the law, the obligation to provide notice is rather vague and limited. The Article 29 Working Party (WP29) tends to highlight the notice obligation in its opinions; however, it sometimes provides contradictory guidelines as to what constitutes an appropriate privacy policy. In general, the WP29 advises developing short notices that should be written in a plain language[4] and be provided directly to individuals in an easily accessible and visible way[5]. At the same time, the WP29 requires that detailed information be provided about data processing practices, which may directly conflict with the requirements of simplicity and intelligibility mentioned above. For example, in several opinions, the WP29 states that organisations 'should provide a comprehensive privacy notice' including all legally required items[6]. In the context of apps and smart devices, the WP29 suggests going beyond the typical notice requirements and addressing considerations such as the proportionality of the data collection in relation to the purposes of the processing, as well as including references related to data retention and security measures[7].

The proposed General Data Protection Regulation puts even more emphasis on privacy policies, extending the existing list of notice requirements included in the Data Protection Directive. It introduces a number of additional elements, such as, providing information about retention periods, the legitimate interests of the data controller (when it relies on the balancing of interests test), contact details of data protection authorities (DPAs), and data transfers. In this respect, the LIBE Committee Report goes even further by suggesting increasing the notice obligations for companies.

Failings of current notices

Privacy policies are certainly beneficial. For example, the requirement for detailed privacy policies has forced companies to start conducting detailed data inventories in order to better understand their processing activities and has thus improved the levels of data protection awareness and transparency among businesses. However, placing so much emphasis solely on privacy policies is not an appropriate response to the issues that we face in today's digitally interconnected world.

Comprehensiveness v. simplicity

There is an inherent tension between the requirements imposed by law and regulators, the current technologies, and the actual data processing practices. In practice, it is difficult to describe, with a good level of precision, highly sophisticated data processing activities in short and an easy to understand way. Then, avoiding the use of technical terminology in privacy policies with a view to make them understandable for the average 'lay man' usually leads to oversimplification of the language. This can result in lowering the levels of granularity which is sometimes seen by regulators as an intention to hide data processing techniques, although in most cases companies' intention is just to provide understandable

information to individuals.

Space limitation

Privacy policies are workable on the internet since it is quite easy to post such documents online and include hyperlinks to allow easy navigation between sections. However, the future lies in mobile and wearable devices. Devices tend to get smaller and smaller, and the size of screens will be reduced or may even disappear. Privacy policies have been criticised in the context of smart mobile devices since mobile apps usually involve the processing of an important amount of personal data and thus require lengthy privacy notice.

However, given that an average privacy policy contains 2,518 words, scrolling and reading the text is practically impossible. In the short term, devices collecting personal data will be ubiquitous and providing detailed notice about data collection on each device will likely become practically impossible and even undesirable for individuals.

Flexibility v. level of detail

In such a fast-moving world, it is difficult to provide detailed information about a company's practices without greatly reducing its flexibility to innovate. Providing detailed information and, for example, listing all data recipients or data fields is often impossible to achieve because of the constant changes of practices. Companies should be accountable for their practices but should also retain some flexibility as to how they will process personal data.

However, companies often face the following challenge: if the notice does not provide sufficient details, it may be seen by regulators as too high-level and thus create potential risks of fines; and if the notice is too detailed, it would reduce its flexibility and require constant updates that may involve going back to individuals and seek new consent for each change in products and services. Both options are not satisfactory and drawing the lines at the right place is certainly difficult to achieve.

Devices collecting personal data will be ubiquitous and providing detailed notice about data collection on each device will likely become practically impossible and even undesirable for individuals

Cost-benefit assessment

Most companies invest a significant amount of time and resources into the preparation of such policies. For example, a large multinational with presence in many different jurisdictions may have to survey all jurisdictions and, instead of one, handle many different versions of the same document to comply with all applicable data protection laws in each country. Moreover, developing a privacy policy does not only put a heavy financial burden on large multinational companies, it might also hinder innovation and affect SMEs.

Start-ups often create innovative products and services that may sometimes pose new privacy challenges and require inventive thinking. However, SMEs often lack the internal resources to prepare appropriate privacy policies that cover each jurisdiction in which they offer their products and services with the assistance from qualified professionals. Therefore, requiring start-ups to prepare comprehensive privacy policies may be an insurmountable obstacle for them while bringing little value to individuals. Finally, the added value of privacy policies for consumers remains unseen. Very little study has been made that systematically assesses what consumers want and what value privacy policies bring to them.

Alternatives to current practices

The rationale behind the use of privacy policies is to safeguard the fundamental right to privacy and to enable individuals to maintain control over the use of their personal data. The idea is to empower individuals and allow them to make informed decisions about whether and how their personal data will be processed. But can they (or even do they want to) make such informed decisions about very technical data processing techniques?

One of the most often cited alternatives to lengthy privacy policies is the use of layered policies, which the WP29 suggests in several opinions. However, the success of layered policies is actually limited. They were first mentioned by the WP29 in 2004 and nearly ten years later, their use is still very restricted. It is therefore doubtful whether layered policies are a solution, or at least it seems clear that they are not the perfect solution.

Another alternative is the use of icons that describe a company's data practices in a simple manner. Icons have been used in other fields and have proven to add value and provide an easy way to inform individuals about the main characteristics of the processing activities. For example, the Creative Commons initiative in the copyright context has proven to be efficient in some instances. The WP29 favours the use of icons, a practice that is also promoted in the proposed General Data Protection Regulation. It would be interesting to watch more initiatives in developing icons and to see whether such use could be generalised.

However, even if the use of layered policies and icons could improve transparency and provide information in an understandable way to individuals, this is not the panacea. We should put more emphasis on the data protection principles, not just on the notice requirements. The focus should be

more on how to effectively protect informational privacy in practice and not so much on whether companies have posted a privacy notice online. Implementing concepts such as privacy by design, privacy by default, privacy impact assessments and other privacy tools, will likely be more beneficial for the society, since it will bring value to companies by improving their internal processes while enhancing trust for individuals and protecting informational privacy.

This trend is partly included in the current EU Commission proposal, but we should go further. For example, the proposed General Data Protection Regulation includes a shift towards more accountability, concepts such as privacy by design and privacy by default, and developing industry codes of practice. In addition, the WP29 discusses the content and importance of privacy policies, but also emphasises the role of developers and engineers[8]. Let us go one step further and avoid following a formalistic approach. When assessing the compliance of certain products and services, let us look at the concept of the privacy policy as one element, among others, and take into account the general compliance context, the product or service lifecycle, companies' internal safeguards, and other tools developed by companies and aimed at empowering individuals.

The illusion of transparency

Privacy policies are not useless; providing comprehensive notice gives the reassuring impression that individuals' privacy is respected. However, a high-level and easy to understand privacy policy accompanied by a number of tools such as lexicons, icons, tutorials, best practices, training videos, explanatory notes, and other privacy toolkits would most certainly empower more individuals than a detailed lengthy privacy notice that will only be understandable by privacy experts.

Regulators feel comfortable that companies comply with data protection law when they disclose a very detailed and comprehensive privacy policy. Additionally, regulators tend to assess compliance with notice requirements in a vacuum, when they should also look at the general context around the products and services such as whether there are other procedures and processes established within an organisation that guarantee individuals' rights in practice.

Too much weight is currently given to the importance of privacy policies when assessing compliance with EU data protection law. Part of the proposed General Data Protection Regulation certainly goes in the right direction, but extending notice requirements would not increase the level of privacy compliance.

Cedric Burton
Senior Associate
Wilson Sonsini Goodrich & Rosati
cburton@wsgr.com

Footnotes:
1. With thanks to Anna Pateraki, Associate, and Lisa Jasmontaite, Legal Intern, at Wilson Sonsini Goodrich & Rosati
2. Article 10 Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. NB - Article 11 Data Protection Directive: the information that needs to be provided slightly differs when personal data are not obtained directly from individuals.
3. Article 2(h) Data Protection Directive
4. Privacy polices 'must be drafted in a clear and simple language that must be understandable by data subjects who have no background in data protection.' WP29 Opinion 10/2004 on More Harmonized Information Provisions
5. 'It is not enough for information to be 'available' somewhere in the website that the user visits.' WP29 Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising
6. WP29 Opinion 6/2007 on data protection issues related to the Consumer Protection Cooperation System (CPCS), Opinion 15/2011 on the definition of consent
7. WP29 Opinion 02/2013 on apps and smart devices
8. WP185 Opinion 13/201 on Geolocation services on smart mobile devices