Data Protection and the Law

Is the Modern Era Conterminous to a Post-Privacy Era?

VANESSA GATT

The notion of privacy is clearly linked to the idea of information flow on the part of the individual himself, who takes upon himself the role of 'gatekeeper', so to speak, determining which information related to their *digital persona* is to be rendered public. Needless to say, both the rise of the social networks phenomenon and the concept of one-to-many communication have deeply altered the traditional notions of privacy, especially when one takes into account the fact that one's ability to control the information that has been shared with others ceases once others make subsequent use thereof. In an era in which millions upon millions of individuals trust social networking sites with highly sensitive data such as addresses, mobile numbers, and real-time location in an attempt to remain in contact with a select number of chosen friends or followers, few are aware of the fact that hiding behind the clicks of a social media website may no longer give rise to absolute protection or non-disclosure of personal data from the law.

This emerges from a recent case against *Twitter* decided recently by the French Courts in which the Social Networking giant was compelled to hand over personal data pertaining to a number of users engaged in anti-Semitic and other such discriminatory activity on the website.[1] The legal battle played out between Twitter, a declared advocate of the right to free speech; and the French Union of Jewish Students (hereinafter rreferred to as 'UEJF'). Although Twitter had already been compelled to remove the incriminating tweets, UEJF made recourse to the French Courts asking that the Defendant Company be called upon to hand over data which would render the individuals guilty of the abovementioned hate crimes identifiable and therefore prosecutable. The implications of this particular case extend themselves to questions of jurisdiction: even though Twitter's servers were physically located within another territory, the French courts still found they had authority to impose local law for activity which had an effect on the French territory itself.

So is the era of social networks, parabolic microphones and spyware also synonymous to a post-privacy era? Not necessarily. Whilst recent international incidents such as the Edward Snowden testimony into abusive American data

[1] Manheim K.M., *J'Accuse Twitter* (Jurist – Forum, 27 March 2013) < http://jurist.org/forum/2013/04/karl-manheim-twitter-france.php> accessed 29 October 2013

collection practices have sparked debate as to the extent to which the fundamental right to privacy must be upheld, an analysis of the current national and European legislation reflects great leaps in the enforcement of data protection legislation. Privacy rights have been recognized as being fundamental at both the national as well as the international level, so much so that the legal instruments seeking to enshrine the enjoyment of this right within the context of civil and political society are numerous. Of particular relevance, however, are the regulations enacted at a pan-European level, which have constituted a propelling force in this particular field of law for a considerable period of time. The debate on data protection and privacy has recently be cast in the spotlight as a result of legal advancements seeking to give rise to a comprehensive approach on personal data protection within the European Union.

The aim of this regulation is to modernize the current data protection rules in order to cater for the ever-increasing technological advances that rendering it easy for personal data to be stored and utilized without the owner's consent, thereby closing off any existent legal loopholes and bettering overall data protection. Despite the fact that debate has been at the heart of the European Parliament's agenda for a number of months, implementation of this Regulation has been countered by a series of deadlocks and delays imposed by the representatives of countries such as the U.K. and Sweden over concerns it will burden and ultimately harm businesses with too much regulation.[2] This is further complicated by the EU-US relations dimension, with the US asking the European countries to slow down the adoption of this Regulation.

Consensus has however been reached vis-à-vis the fact that the enactment of the Data Protection Regulation is of the utmost expediency. Policy makers around the globe must ensure that informational self-determination ranks highly amongst the issues requiring prompt legal action in order to be able to overcome the alarming threats of privacy deprivation. Perhaps the situation at hand was best summarized by Karel De Gucht, Deputy Prime Minister and Minister of Foreign Affairs of Belgium who recently stated that State security and privacy are 'all too often presented as dichotomous rivals to be traded-off in a zero-sum game. However responsible, liberal and democratic policy makers do not have the luxury to balance one against the other. Both are needed'.[3]

---

[2] Bodoni S, *Privacy Chief Warns EU Over Data-Law Delay Amid U.S. Spying* <http://www.bloomberg.com/news/2013-10-30/privacy-chief-warns-eu-over-data-law-delay-amid-u-s-spy-scandal.html> accessed 29 October 2013

[3] De Gucht K, *Re-Inventing Data Protection?* (Springer Publications, 2009), p. 5