French privacy laws and the use of personal or professional devices at work

By Christophe Héry and Jean-Christophe Guy

The issue of the boundary between the private and professional lives of employees using their own or their employer’s devices for professional purposes was addressed, in France, in early 2015, first by France’s highest civil court ruling on the use of devices supplied by employers, and then by the French data protection agency, (Commission Nationale Informatique et Libertés - CNIL), which issued guidelines for the “Bring Your Own Device” approach.

Privacy and the use of professional devices

In a ruling of 10 February 2015, the commercial division of the Cour de Cassation found that the employer had a right of access to the text messages which their employee had sent and received by SMS (“Short Message Service”) using the mobile phone provided by the employer under the employment contract – even in the employee’s absence.

Although article 9 of the French Civil Code sets out the principle according to which everyone has a right to privacy – even at the workplace, as is generally recognized, the right of privacy did not prevent the production of the disputed text messages because the Cour de Cassation found that “text messages sent or received by the employee using the telephone provided by their employer for work purposes are presumed to be professional in nature”.

This is the same solution as was chosen for folders and files created by employees on their hard disk drives and then extended to internet connections, browser bookmarks, and e-mail.

Still, it is not an irrefutable presumption as employers may only access their employees’ messages which are not identified as personal. However, the practicalities of identifying messages as personal is problematic where text messages are concerned as they do not include any “Subject” field, so that employees are encouraged to start the message with the word “Personal” or to identify SMS contacts as private. Therefore, employees may determine their privacy sphere themselves.
Even though a text message may be identified as “personal”, the employer may still take cognizance of its contents in the employee’s presence or after duly summoning the latter.

Privacy and the use of personal devices
Under the BYOD approach, employees use their own IT tools for professional purposes. Although the BYOD model appears to find favor with employers and employees alike, it raises many issues relating to both the security of businesses’ data and IT systems and the employees’ right of privacy. The CNIL (the French DPA) in a communiqué released on 19 February 2015, issued guidelines for the use of personal IT equipment in a professional context.

The CNIL reminds that under French labor law, all employers have a duty to provide their employees with the means to perform their employment contracts. Therefore, the use of personal devices for professional purposes can only be subsidiary in a professional context. Furthermore, where employees are to use their personal devices for professional purposes, their consent is required.

- Reconciling conflicting imperatives
As regards the minimization of data security risks, the CNIL first recommends identifying such risks according to context (e.g., type of equipment used, nature of data concerned) and then classifying them according to severity and likelihood.

Furthermore, employers are invited to determine which security measures they should implement and to formalize them in an appropriate security policy. Employers must in all cases abide by the proportionality principle.

As regards the employees’ right of privacy, the CNIL recalls that employers may not implement security measures that aim to or in effect restrict the use of a device for personal purposes on the grounds that the device can be used to access the company’s resources.

Moreover employers may not access the private data stored in the personal areas of their employees’ devices either. Likewise when a remote wipe system is set up by employer, such a system cannot be used to delete all data stored on the employee’s personal device indiscriminately.

- Technical and HR challenges
From a technical standpoint, employers must be able to separate personal from professional data, even more so if they have remote access to their employees’ devices.

In terms of human resources, employers implementing a BYOD model must devise awareness-raising tools, but also tools to monitor and where necessary to sanction employees using wrongfully their personal devices for professional purposes.

Footnote
1Cour Cas., com. Div., 10 February 2015, no. 13-14779, FS P + B

2Cour Cas., labor div., 17 May 2005, no. 03-40017; 18 October 2006, no. 04-48025

3Cour Cas., labour div., 09 July 2008, no. 06-45800.

4Cour Cas., labour div., 09 February 2010, no. 08-45253.

5Cour Cas., labour div., 15 December 2009, no. 07-44264.

6www.cnil.fr/documentation/fiches-pratiques
Foreign investment in online retail companies in India

By Ajit Sharma

Online retailing in India has seen unprecedented growth rates in the last five years increasing from about $4 billion in 2009 to about $25 billion in 2015 and expected to increase to about $100 billion by 2020, according to various studies. Several e-commerce start-ups have benefitted from this surge in growth and many commence operations every month.

While growth in start-ups has largely been fueled by change in customer preferences, i.e. many of India’s about 250 million internet users are today open minded about purchasing online, and due to cash for delivery schemes employed by most e-commerce portals, the availability of relatively easy funding from private equity firms has played an important role in India’s internet revolution.

A number of US based private equity funds and investors have since invested in Indian e-commerce companies. And although the laws regulating foreign investment have simplified immensely over the past few years, legal counsel at or prior to the term sheet stage is imperative to invest in e-commerce companies in compliance with India’s foreign direct investment ("FDI") laws.

Multi-brand retailing is a politically sensitive issue in India and various think tanks are of the view that foreign investment should not be permitted in large retail stores selling multi-branded goods since it would throw out of business millions of mom and pop stores in Indian cities. Perhaps for this reason, FDI in e-commerce companies is regulated to partly ensure that such companies do not indirectly carry out sales of multi-brand goods to consumers in India.

Current FDI laws permit 100% foreign investment without any approvals from any Indian regulator, i.e. on automatic route, in e-commerce companies, which do not sell directly to consumers or end users of goods. Such companies typically are a marketplace where buyers meet consumers and sale invoices are issued by the seller instead of the e-commerce company. 100% FDI is allowed in e-commerce companies engaged in Business to Business ("B2B") sales, since sale is not made to an end user and hence is not multi-brand retailing in strict sense of the term. Thus often e-commerce companies engaged in Business to Customer ("B2C") and B2B sales have to restructure prior to receiving FDI so as to ensure that they do not carry out any B2C transactions.

One expects that in the coming year the government will lift the restrictions on foreign investment in B2C e-commerce companies for these restrictions may needlessly limit the growth of online retailing industry in India, which generates huge revenue for the state and provides employment to thousands of people.

Mr. Ajit Sharma is an advocate on record in the Supreme Court of India and is qualified as solicitor in England and Wales. sharma.ajit@rhalegal.com
Drones and Privacy: Is Big Brother airborne?
By Steven De Schrijver and Thomas Daenens

Until a couple of years ago, drones, or remotely piloted aircraft systems (“RPAS”), were only used for military purposes. Recently, however, the technology has been further developed, as a result of which drones have not only become smaller, more practical and less expensive, they can and are also used for civil or commercial purposes, such as infrastructure monitoring, photography or even transport of goods and people. While no one seems to question the potential social and economic benefits of drones, in particular as regards jobs and growth, their use by private companies and individuals for economic or other purposes does raise a number of important concerns.

In Belgium, as in most European countries, there are no data protection laws or regulations that relate specifically to the collection and processing of personal data through the use of drones. There is no question, however, that the personal data collected by drones is also protected by the existing data protection legislation in Belgium and the EU. The Belgian Privacy Commission (the Data Protection Authority) confirmed this point of view in its Advice dated 22 July 2015 with respect to a draft Royal Decree regulating the private and commercial use of drones proposed recently by the Minister of Transport. The Royal Decree itself also states that users of drones must ensure compliance with applicable data protection laws.

Under the applicable data protection rules, the use of a drone will always require a legitimate ground for processing. This can be, amongst others, the unambiguous consent of the data subject or the necessity of the processing for the execution of a contract or for compliance with a legal obligation. In the context of recreational or commercial use of drones, consent will in most cases be the only legitimate ground available, although it may be impossible or at least very difficult to obtain.

The Privacy Commission also points out that the use of cameras on drones for surveillance purposes is subject to the Act of 21 March 2007 on the use of surveillance cameras. Pursuant to this Act, cameras placed on drones are to be considered mobile cameras, which may only be used by law enforcement authorities for the purpose of crowd control or license plate recognition.

Applying and enforcing the data protection regulations to a potentially highly intrusive new technology is very important, but at the same time it will likely not be easy.

Drones are by nature mobile and discrete, and in particular the smaller and lighter drones flying at relatively high altitudes but equipped with powerful cameras or recorders, will be very difficult to detect. And even if drones are used in a visible and indiscrete way, the question remains... (continued on p.5)
...how one can enforce the privacy regulations (in particular information and consent) in practice. The Data Protection Authority also pointed this out in its Advice related to the Royal Decree, but it did not offer any solutions.

Therefore, in order to ensure privacy protection to the greatest possible extent, it is recommended to take the necessary measures from the outset, which leads us to privacy by design.

Drone manufacturers should be invited to analyze at the earliest stages of development how their device might interfere with the privacy of individuals, so that they may then build these devices in a way which reduces such interference to what is strictly necessary and proportionate to the purpose pursued. As such, manufacturers might propose different types of sensors depending on the purchaser’s objective, so that the latter may choose the one that is least intrusive (for example, if the drone is used to build accurate roadmaps, it does not need high resolution cameras able to read license plates). Drones could also be equipped with tools that provide for automatic masking of private areas and automatic detection and pixilation of faces that are (accidentally) gathered in images and videos. Manufacturers could also be encouraged (or forced?) to set up data retention by design, that is to say, the possibility to schedule the automatic and regular deletion of the data processed.

Obviously, even if drones are designed to protect privacy and are equipped with all possible tools to ensure compliance with applicable law, their owners should also be made aware of their obligations. Drones should therefore come with clear information about the applicable privacy rules and the different obligations of the user under national and EU law.

As drone use for commercial or recreational purposes is still in its infancy, it remains to be seen how their use will impact people’s privacy and to which extent the data protection regulations will be enforced in practice. Especially in the first years to come, data protection authorities and courts will need to be vigilant and show that non-compliance cannot be tolerated.
PEDS Mission Statement

The Privacy, E-Commerce and Data Security Committee has been established as a resource to assist in the education of international law practitioners on the evolving international laws and practices relating to privacy and data protection, in particular as they relate to global e-business, and to contribute to the development of policy and the promotion of the rule of law in those areas.

PEDS Committee News

- PEDS Committee Co-Chair Gregory Voss recently spoke on “Security and Privacy Implications of e-Procurement in TTIP” at CIDOB (Barcelona Centre for International Affairs)’s seminar on “TTIP negotiations: caught between myth and reality?” CIDOB is the top-ranked think-tank in Spain, and 15th ranked in Western Europe accorded to the highly-cited 2014 Global Go to Think Tank Index Report of the University of Pennsylvania. In addition, Voss is co-author of the updated “Chapter 9: E-Compliance” in recent loose leaf supplements (e.g., 2015-2 Supplement) to Theodore L. and Frederick Z. Banks’ Corporate Legal Compliance Handbook, Second Edition, published by Wolters Kluwer Law & Business.

Your contributions are always welcome!

Thank you, everyone for participating in our 2015 Summer Edition PEDS Newsletter and please do not hesitate to give feedback to or submit articles for the next edition to: youyoung1110@gmail.com.

You are welcome to submit an article for the next edition, 2015 Fall Edition PEDS Newsletter will be due 11/15/2015. Below are the formats:

- **Topics**: any aspect of international or comparative issues in privacy, e-commerce and data security law are welcomed.

- **Author**: Contributors will be identified by name below the title. The author credit will contain the author’s name, law firm or other association. (The authors are suggested to accompany the article with short profile)

- **Citation**: Keep citation to a minimum. Use endnotes and the Bluebook format when necessary.

- **Content formation**: The use of text boxes, tables, graphics or other illustrations relating to the article topic are encouraged.

- **Length**: 100 and 350 words. 1-3 sentence summaries of already published article with links to article, providing no copyright issues involved, are also accepted. Text should be single spaced, with one-inch margins.

- **Title**: Please include a suggested title for your article at the top of the page.