SOCIAL MEDIA: WHO OWNS YOUR BRAND ?

« You no longer own your brand. Your customer owns your brand. »
(Jeremiah Oywang)
« A brand is no longer what we tell the consumer it is. It is what consumers tell each other it is. »
(Scott Cook)

I Introduction: What can go wrong (1) ?

Social media is no new phenomenon. For the best part of a decade people, businesses and consumers have harnessed the internet to aid communication. While initially a social device, most businesses and industries now recognise the ubiquity and commercial power of networking. Organisations seeking to profit from a smaller, smarter planet can engage directly with both existing and future consumers.

Between 2010 and 2011 Facebook saw an approximate 40 % rise in daily usage. Today businesses can speak directly to over 640 million Facebook users. Twitter, too, presents an opportunity for companies to hone their message, with over 175 million reading, and contributing, to person-to-person and business-to-consumer dialogue. Companies no longer rise and fall solely on traditional 'word of mouth' brand development. Its modern equivalent is 'going viral': the ability of a brand not just to contribute to, or influence, a conversation, but instead be that conversation.

This involves articulating a message across numerous platforms, often simultaneously, combining traditional marketing with modern, nuanced methods through online and mobile technologies. Opportunities abound, but with increased risk as businesses place the voice of their brand in the mouth of the customer. How can businesses moderate what is said about their brand? Can companies and users enforce often untested online legal rights ? As social networking and content consumption grows, how can organisations exert control? In an at times bewildering maze of data, technology and opportunities, businesses need to consider not only what message they want to articulate for their brand, but who, ultimately, owns that brand and controls its use ?

A. Control

Harnessed correctly, social media can help to define and revitalise brands, bringing products and services into the public eye and allowing consumers to engage directly with the company. However, social media content also creates an issue of control. Businesses have to learn techniques to ensure that it is the correct message which sticks in users' consciousness.

Optimising a brand through social media involves a significant amount of planning and development. Firms might, for example, try to humanise their brand through incorporating user-generated content (« UGC ») into official publications and websites, encouraging conversations and employing key term recognition algorithms in arrangements with search engines and advertising networks.

Twenty-first century technology and communication is inherently pro-social, breaking down boundaries between people, communities and organisations, disseminating and proliferating thoughts and ideas. Brands have to engage in social networking in the same style as their customers. By being part of a conversation they can help mould and shape it, influencing and controlling it by employing the same networking language and behaviour as individuals. Humanisation is key for organisations, making their products and brand fit seamlessly into a wider network. In this way, brand messages are entrusted to the consumers, and companies are investing in this. According to the Internet Advertising Bureau (« IAB ») (2), in the first half of 2011 companies spent £2.3 billion on internet advertising, up 14 % on the year previously. Organisations look to harness what people say about a brand and use positive energy attaching to it across social media platforms to secure goodwill. This use of brand 'ambassadors' helps organisations exercise a level of control over public content.

This might take the form of networking tools set up on official product websites, giving the owner full control over UGC. The purpose is twofold: to add a networking dimension to the user experience, allowing the consumer to play a role in the process; and to speak to those who have not yet made up their minds and are seeking further information. Ford Motor Company, for example, set up the 'Ford Story'. This allows consumers to upload personal stories to a Ford-run and operated platform within Ford's official website. Users are encouraged to upload stories about the symbiosis between a life event and a Ford purchase : « Personal stories make the Ford Story as individual as you are. » Here, Ford manages the content and the message, while simultaneously contributing to a broader social networking discussion.

The Ford example above illustrates internal networking within a company's official website, governed by specific user guides. External networks provide less comfort for brand holders, however. It is hard to control content on unmoderated sites where free information creates both opportunity and risk. Without observation and moderation, negative and occasionally libellous comments can seep into newsfeeds and comments. On an official moderated forum such a situation is embarrassing but brief, or non-existent where good pre-moderation is in place. On public forums not directly controlled by the company, a brand being left solely to the general community can backfire if

(1) Written by Iain Stansfield with the collaboration of Robert Samuelson.

(2) « First Half '11 Internet Advertising Report » published by the IAB in conjunction with PwC on 28 September 2011.

content is not properly observed and when necessary removed.

Organisations that facilitate social networking often have philanthropic principles at their core : knowledge is power, information is free, dialogue breaks down walls across and within communities. But they are also businesses in their own right, and are often free to access through sale of their advertising space, which is at a premium. Banner ads and sidebars use ad-serving technology and search term recognition algorithms which harness information that individuals enter into social media sites in order to create targeted adverts served when that individual is on the site. A user's profile can produce a highly specific picture of their age, location, family, gender and interests. Adverts for relevant products can appear on the side of the screen viewed by that person when they are viewing or participating in groups dedicated to a particular competing brand. For companies seeking to profit from social media's technological advances there can therefore be benefits and dangers: on the one hand enjoying mass marketing through social platforms; on the other potentially victim to a networking hijack from a competitor piping ads at its users.

B. Influencing the chatter

How can a business influence brand conversations? We have already looked at the dilemma caused by brand-controlled sites as opposed to more user-led forums, and in particular the trade-off between more controlled 'on-message' branding against more 'organic' but less reliable messaging. The debate on whether to moderate UGC is not merely one of brand management and credibility, however. It can affect legal liability.

Article 12 of the E-Commerce Directive (EU Directive 2000/31/EC) (the « Directive ») states that providers of an online social media service will not be liable for content published as long as they did not initiate or deliberately modify the publication. The decision to monitor content can therefore bring with it a surrender of the shield from liability for users' publication of unlawful comments on one's site (perhaps defamatory or infringing intellectual property rights).

External reputation management firms, combining public relations, advertising and media law skillsets, can help to ensure that where monitoring is undertaken it is effective. Tempero Social Media Management, according to CEO and Founder Dominic Sparkes, monitors millions of messages for over sixty clients across fifty platforms in fifteen languages. Sparkes, in a recent paper on social networking, argues that firms must consider a variety of issues when attempting to influence brand conversations. Are message posts libellous or breaches of privacy ? Are there contempt of court questions ? In reprocessing UGC, or 're-tweeting' on Twitter, is the company forgetting competition and intellectual property obligations ? Will it constitute a marketing promotion under the Advertising Standard Authority's Regulations ? There are a myriad of concerns. Businesses have to be able to deal with matters as they arise, often through external reputation management advice.

Brands will sometimes intervene more directly in social media discussions of their products and services, at the risk of legal sanctions. Handpicked Media Ltd (« Handpicked ») operates a blogging network, compiling content that their bloggers have created and publishing it across a number of social media platforms. The Office of Fair Trading (« OFT ») (which monitors content across social networks in order to check that publications from companies comply with the Consumer Protection from Unfair Trading Regulations 2008 (« CPR ») took enforcement action in December 2010 against Handpicked under the CPR. Handpicked was found to have breached regulations 3(4)(b) under provisions of regulation 6 of the CPR, and paragraph 11 of Schedule 1. Under regulations 3(4)(b) and 6 unfair commercial practices are prohibited. Regulation 3(4)(b) states that a commercial practice is unfaire if « it is a misleading omission under the provisions of regulation 6 », which includes misleading omissions of importance that « causes or is likely to cause the average consumer to take a transactional decision he would not have taken otherwise ». Schedule 1 adds that it is unfair to use editorial content in the media to promote a product in situations where a trader has been paid for the promotion, without making this clear (3).

The OFT found that Handpicked had not made it clear that companies were paying it to engage bloggers to create promotional content. Handpicked undertook not to repeat what the OFT considered to be unfair conduct, agreeing to identify when promotional comments had been paid for in future (4). The heart of the action, and the relevance of the CPR, is to resolve situations where ordinary social networking users might end up making a transactional decision that they may not have made had they known an external agency had been engaged to create the content.

The OFT's action against Handpicked was the first of its kind. As a result, promotional material must clearly state when content has been paid for. A wider issue is the legal and public relations risk of a business employing third parties to masquerade as consumers and ending up with an OFT sanction. Businesses should in that context be wary of paragraph 22 of Schedule 1 of the CPR, which states that it is unfair if a trader falsely represents itself as a consumer. This might occur by a business posting its own reviews on a website. A blog written by an individual employed for the sole purpose of writing promotional material about that business may therefore be contrary to the CPR unless clearly labelled.

C. Crowdsourcing

Some businesses are exploring new methods of creating brand loyalty without using social networking platforms. 'Wikification', harnessing user ideas to give consumers a sense of ownership of brands of businesses, has crystallised the crowdsourcing debate between 'legal' and 'social'. Empowering consumers to contribute content directly to a brand helps expand the relationship between business and consumer. Simultaneously, intellectual property concerns and terms of use requirements can countervail.

Incorporating user ideas into new products and plans for a business through a controlled social networking site is illustrative of crowdsourcing. One large multinational food and beverage company recently created a site that encourages users to contribute new ideas and comments for the company to consider. Through this the business gives consumers a stake in brand development, establishing a networking experience that can be easily monitored, whilst benefiting from creativity from the people it most wants to be close to. New product lines, ideas for how stores

(3) http://www.legislation.gov.uk/uksi/2008/1277/pdfs/uksi_20081277_en.pdf

(4) http://www.oft.gov.uk/OFTwork/consumer-enforcement/consumer-enforcement-completed/handpicked_media/

can be fitted out and promotions all come from users who have to sign up to take part, allowing the business to monitor numbers, content and who their customer is: key demographic information vital for future plans.

There are, however, two sides to such initiatives. There is the outward, societal face where users can « share, vote, discuss, see » and an internal aspect of dense legalese and restrictive terms and conditions thrown off by corporate concerns about intellectual property ownership. Terms of Use can end up becoming lengthy documents, granting, as one example sets out, « a perpetual, irrevocable, non-exclusive fully-paid up and royalty-free license to use any ideas, expression of ideas or other material you submit… without restrictions of any kind and without any payment or other consideration of any kind, or permission or notification, to you or any third party ». The business controls ideas once submitted. Such restrictions are legally desirable for the business to assert full control over a profitable idea, but use complex legal terminology arguably at odds with the spirit of the engagement and (for those who read it) off-putting for the users. Legal best practice and social engagement may not be aligned.

D. Gamification

Some marketing specialists have devised a more nuanced approach to brand development through social media. Gamification, disseminating content about a brand through a user-driven game-based platform, is emerging as an interesting option. By creating a platform that allows users to communicate with each other about a brand, alongside earning rights and privileges to discover more content, businesses can play an interactive sleight of hand. Consumers are placed at the heart of a brand-based gaming experience, creating an artificial sense of user empowerment. In reality, the business still controls the platform, of course. Gamification shows brands drawing on people's natural competitiveness and, at its smartest, making consumers of them in the very process of their playing the game.

This technique has been employed across a number of industries. The Kaiser Chiefs allowed fans of the band to pick and organise their new album tracklisting. J.K. Rowling's 'Pottermore' website will bring new Harry Potter material, information and products to users by encouraging reading development. 'SCVNGR', a Google Ventures-backed enterprise, involves users playing challenges across different locations to score points. Organisations engage SCVNGR to build the game layer by adding their own challenges to relevant locations.

Nike introduced a device in conjunction with Apple called 'Nike+'. Users can work on their physical fitness by completing aerobic challenges and synching their data between devices. Nike's name in conjunction with an exercise application creates brand association for a demographic group most apt to buy their products.

The Outnet's 'Stylecred' iPhone application is a broader example. From the makers of Net-a-Porter, Stylecred users create and share looks with their friends. By getting new friends to sign up, current users win 'points' (in the form of store credits) to be redeemed at the official Outnet store. In this way, Net-a-Porter is encouraging brand association while adding a competitive element to increase consumer numbers.

Of course, in employing gamification techniques businesses must be wary of the legal framework around e-commerce and gaming. Consumer rights in relation to payment protection and cancellation, sale of goods and supply of services legislation, consumer credit obligations, e-commerce, competition and regulatory law and gambling rules all apply and may differ from state to state. This can be particularly problematic for cross-territory gamification formats, and if not managed well can throw up a thicket of legal complexity around what should for its users be an easy, unengineered experience.

E. The balance

For lawyers, it is perhaps most convenient to look at the legal challenges thrown up by brands engaging with social media from two angles.

First, there is the probably self-evident (to lawyers) fact that social media does not exist beyond the law. For businesses engaging with social media, both mainstream law (commercial, intellectual property and much else), as well as those laws particular to marketing and promotions, apply. Beyond the basic need for businesses to be compliant in all platforms of customer engagement, these laws are also there to assist businesses in asserting and retaining ownership and control of their brands.

Second, there is the overarching need to understand that a forceful approach to legal practice and enforcement will often not be appropriate. The user impact of a social media-led campaign may suffer if it is encrusted with terms and conditions and other 'legal' material. A light, strategic approach is required. It is also important to be aware that the repercussions of legal action within the social media sphere can be unduly felt. A letter before action could be released to a blog and be there for all to see, causing potentially greater damage to a brand than the mischief of which it was complaining. A community of 'brand ambassadors' can be angered and alienated by a heavy-handed legal approach.

II Trademarks in social media (5)

The popularity of social media is a double-edged sword for trademark holders (« TM holders »), who may benefit from the increased exposure of their trademarks on Social Network Sites (« SNS »), but who must also deal with the threat of trademark infringement by the users of such websites.

Since the development of Web 2.0. companies are able to reach a wide audience using a small fraction of traditional advertising budgets. Marketing on the world wide web ("E-marketing") also has the advantage of measuring statistics easily and inexpensively.

But everything has two sides, and so does the use of social media. Having consumers communicate about brands is of benefit to companies, but what if consumers engage in improper or unauthorised trademark use? A TM holder will probably not be pleased to find out that a Facebook user obtained a Facebook URL that contains its trademark or a Twitter account with its trademark. This chapter sets out these threats and the potential remedies available that can limit the risks of using SNS, and thus allow a TM holder to harness the benefits of social media at its best.

Dealing with the threats of SNS can be preventative or repressive. Prevention comprises all measures a TM holder can take to prevent those threats from coming to pass whereas repression comprises the measures a TM holder can take when a damaging act (e.g. trademark infringement) has already occurred.

(5) Written by Christine De Keersmaeker with the collaboration of Willem-Jan Cosemans.

A. Prevention

To make effective use of the benefits offered by SNS without being exposed to its threats, TM holders should register their trademark or username and identify interesting sub-domain names (see below). They should create their own pages or fan sites on SNS. TM holders should monitor the use of their trademarks on SNS. The most common way of doing this is to use search engines (Google Alert). External monitoring service companies or a "web chatter" listening service are other excellent options should search engines not suffice. TM holders should also launch marketing campaigns on a regular basis in order to educate the public about the ownership of their trademark. It is important to continue to educate and remind the public that a trademark is an important signifier of the TM holder's quality products and/or services. Create or revise your trademark policy. Tell your customers that you have a trademark so that it can be the subject of conversation. Inform your own employees. Finally, TM holders should keep a record of all action taken to ensure demonstration of proper control of the trademark should it ever come in use or be required in the future (6).

Most importantly however, TM holders should identify the sub-domain names they want to obtain through SNS before they are obtained by third parties. The Uniform Domain Name Dispute Resolution Policy (« UDRP »), which governs trademark-based domain name disputes, only addresses trademark infringements in second-level domain names (e.g., « facebook » in www.facebook.com) and does not address the sub-domain names, known as the vanity URL's. This means that a TM holder cannot stop unauthorised use of its trademark in a personalised Facebook sub-domain (e.g. www.facebook.com/trademark) by relying on the enforcement procedure of UDRP. TM holders should therefore identify the sub-domain names they want to use and register these. This means registering existing trademarks but also future names of key products (e.g. iPhone 5, 6, 7, etc.), in order to avoid problems in claiming back those sub-domain names in case they have been registered and/or used by a third party.

Claiming back sub-domain names and other repressive measures can moreover be harmful to the image of the TM holder. « Hard measures » do not always lead to the desired results. Coca-Cola for instance adapted « soft measures » and with success. The Coca Cola Facebook page for example wasn't created by Coca Cola itself, but by two Coca Cola fans in Los Angeles. The two were contacted by Coca-Cola, who asked them to partner with Coca Cola to manage the page, a move that showed a gracious approach to social media by the TM holder, and the page is now the second most popular page on Facebook (7).

B. Repression

Even once all possible preventative measures have been put into place, they may not be sufficient in order to address trademark damage. Legal actions may have to be considered.

The question however is whether trademark laws address the issues presented by SNS. They usually do in principle, but with certain difficulties. In principle trademark laws apply to all forms of use including use on SNS.

When a TM holder discovers that a third party has registered the holder's trademark as a sub-domain name on a social media website, it might be a straightforward issue of a trademark infringement. In such cases it may be possible to launch trademark infringement proceedings based on the provisions of traditional trademark legislation. Most SNS however offer tools for TM holders to address such infringements, so TM holders do not always have to waste considerable time and expense on traditional trademark infringement proceedings. We would consider the latter proceedings as being « hard repression » and using the SNS policies to address the trademark infringement as being « soft repression ». The message is to not immediately overreact to a trademark issue on a SNS.

1. *Soft repression: Policies of SNS*

SNS use their own definitions for what constitutes a trademark infringement. These definitions of « trademark violation » are often broader than the definitions used in traditional trademark legislations.

Twitter for example describes a « Trademark Policy Violation » as follows: « *Using a company or business name, logo, or other trademark-protected materials in a manner that may mislead or confuse others with regard to its brand or business affiliation may be considered a trademark policy violation.* »

When Twitter receives reports of trademark policy violations from TM holders, Twitter engages in reviewing the account (i.e. sub-domain name) and may take appropriate action.

When reviewing such reports, Twitter places a lot of importance upon the intention of the third party. If the third party intends to create confusion on the part of the public, Twitter engages in the suspension of their account, and in cases where the intention of the account holder has not been established, Twitter gives the account holder the opportunity to clear up any potential confusion (8). In this respect, it must be stressed that using another's trademark in a way that has nothing to do with the product or service for which the trademark was granted is not a violation of Twitter's Trademark Policy (9).

Therefore, more complex cases involving the use of a trademark with a reputation in connection with dissimilar products or services could still require recourse to the courts (10).

Twitter also has a separate « Impersonation Policy » and « Name Squatting Policy ». In these policies, the intention to mislead is again a key issue but Twitter will only release inactive or squatted usernames in cases of trademark infringement.

Impersonation is pretending to be another person or entity in order to deceive (for example, TonyLaRussa/Twitter 2009 : Anthony La Russa, manager of

(6) For an analysis of the value of such evidence see: J. Lorré, « Facebook en arbeidsrecht: mysterium tremendum et fascinans », *R.W.*, 2010-11, 1507-1510.

(7) See : http://www.insidefacebook.com/2009/03/18/how-do-you-treat-a-fan-who-owns-your-facebook-page/.

(8) Twitter Trademark Policy (available at http://support.twitter.com/articles/18367-trademark-policy) : « When there is a clear intent to mislead others through the unauthorized use of a trademark, Twitter will suspend the account and notify the account holder. When we determine that an account appears to be confusing users, but is not purposefully passing itself off as the trademarked good or service, we give the account holder an opportunity to clear up any potential confusion. We may also release a username for the trademark holder's active use ».

(9) Twitter Trademark Policy (last accessed, October 2011).

(10) K. Cullen and A. Mallon, Social-Networking sites: opportunities and challenges for brand owners, in *World Intellectual Property Review Annual 2011*.

the St. Louis Cardinals, sued Twitter after an unknown Twitter user created an account at twitter.com/TonyLaRussa and pretended to post updates as La Russa. The fake Twitter page included La Russa's photo and a handful of vulgar updates. Only one line of the « profile » suggested it was all a fake : « Bio Parodies are fun for everyone »). Name Squatting is use of a user name with the deliberate intent to profit from goodwill belonging to someone else (for example with Heinz, where someone decided to see what happened if he became a Twitter squatter. It took Heinz two weeks to notice the account and to eventually have Twitter change the account name. This is an excellent example of the potential consequences of a lack of monitoring.)

Facebook also provides an « automated IP infringement form » which a TM holder can use to report a trademark infringement by a Facebook user. Facebook provides special provisions for name squatting : « *If we determine that usage of a username is for squatting, that username will be reclaimed by Facebook* ». Unlike Twitter, no exception for non-trademark infringements is provided. Hence, it appears that Facebook's « Name Squatting Policy » goes further than Twitter's.

There's no doubt that the above mentioned procedures are extremely valuable tools against trademark infringements which may also help the SNS to avoid possible allegations of infringement. Therefore, when a TM holder discovers that a third party has registered the holder's trademark as a sub-domain name on a social media website, before immediately resorting to traditional trademark legislations, he should first check the trademark violation policies of the website at hand.

2. *Hard repression: current trademark laws*

Soft measures may not be sufficient to address trademark infringements, in which case the hard measures may be necessary. The question then is whether the trademark laws address the concerns and who can be sued. This will not necessarily be the SNS. Most of them will argue that they are shielded from liability because they were not the party involved in the creation of the infringing content. That argument has often been upheld (for example TonyLaRussa : It was only hours after the lawsuit was filed that Twitter removed the fake La Russa page and its postings). The current EU Trademark Directive and Regulation can however provide TM holders of EU Member States with powerful tools for « brand image protection » against the account holder :

- Article 5(1)(a) CTMD and Article 9 (1)(a) CTMR regulate protection in cases of double identity – a sign identical to the protected trademark used for identical goods or services. In this regard, the CJEU holds that, besides the essential function of indicating origin, a trademark's quality, communication, investment and advertising function enjoys absolute protection under the above mentioned articles.
- Article 5(1)(b) CTMD and Article 9 (1)(b) CTMR regulate protection in cases of double identity and/or similarity – a sign identical or similar to the protected trademark used for identical or similar goods or services. Additionally, a likelihood of confusion must be established.
- For reputed trademarks Article 5(2) CTMD and Article 9(1)(c) CMTR provide TM holders with an enhanced protection against dilution.

TM holders must overcome several hurdles however in order to successfully invoke the above provisions to cease the use of their trademarks on SNS. The use of a trademark on a social media website shall not always constitute a « use of a trademark » within the meaning of the above mentioned provisions. Moreover, it shall not always be possible for the TM holder to establish an infringement within the meaning of these provisions. And last but not least, many territorial problems can arise, since most SNS are accessible worldwide, while trademark rights remain limited by territory.

(i) The use of trademarks in social media

SNS have developed new forms of use in recent years (e.g. an unauthorised fanpage using another's trademark).

The use of a trademark on a social media website will often probably not constitute a use within the meaning of EU trademark legislation since the use of a trademark as a rule can only be invoked against economic operators and not against individuals (11). An individual operating a fanpage while using the TM holder's trademark without authorisation will therefore not be concerned.

However, in the Google France case about keyword advertising, the CJEU held however that a sign selected by an advertiser as a keyword in the context of an internet referencing service constitutes a use by the advertiser in order to trigger the display of its advertisement and is thus a use in the course of trade (12). For economic operators therefore the use of a trademark in the course of trade is thus withheld with ease by the CJEU.

This use has an adverse effect on the function of indication of origin of the trademark. That function is essential for the trademark and should be protected everywhere including on SNS. The additional protection against dilution justified by marketing efforts and investment (mostly in cases regarding « reputed marks ») has often lead to an extension of trademark protection to other uses.

The CJEU has not set high requirements for « use in the course of trade » (13) and « use in relation to goods or services ». The latter condition in particular is applied flexibly by the CJEU (14). As a result, this requirement does not prevent TM holders from asserting their rights against references to their trademark even though the public does not perceive these references to be an indication of commercial source. Use of a trademark in the form of a reference is thus brought within the reach of the exclusive rights of TM holders. According to the German Federal Court of Justice (15) even decorative use constitutes relevant trademark use on the basis of CJEU jurisprudence.

That extension, if invoked for use on SNS may lead to the endangering of the fundamental freedoms of expression.

(11) C.J.E.U., 12 July 2011, C-324/09, *L'Oréal/eBay*, para. 54.
(12) C.J.E.U., 23 March 2010, cases C-236/08-238/08, *Google France and Google/Louis Vuitton et al.*, para. 49-52.
(13) See: C.J.E.U., 23 March 2010, cases C-236/08-238/08, *Google/Louis Vuitton et al.*, para. 50; C.J.E.U., 11 September 2007, case C-17/06, *Céline/Céline*, para. 22; C.J.E.U., 12 November 2002, case C-206/01, *Arsenal/Reed*, para. 40.
(14) See: C.J.E.U., 23 March 2010, cases C-236/08-238/08, *Google/Louis Vuitton et al.*, para. 71; C.J.E.U., 23 February 1999, case C-63/97, *BMW/Deenik*, para. 42; C.J.E.U., 12 June 2008, case C-533/06, *O2/Hutchison*, para. 35-36.
(15) German Federal Court of Justice, 3 February 2005, case I ZR 159/02, www.bundesgerichtshof.de.

(ii) Infringement or not?

a. Art. 5(1)(a) CTMD and 9(1)(a) CMTR

Established case-law of the CJEU holds that a TM holder cannot oppose the use of a sign identical to their trademark if that use is not liable to cause detriment to any of the functions of that trademark (16).

Those functions as we mentioned above include not only the essential function of the trade mark, which is to guarantee to consumers the origin of the goods or services ('the function of indicating origin'), but also its other functions, in particular that of guaranteeing the quality of the goods or services in question and those of communication, investment or advertising (17).

With respect to these trademark functions under art. 5(1)(a) CTMD and 9(1)(a) CMTR, the CJEU stated in the above mentioned Google France case, that using another's trademark as a keyword for one's own advertising did not have an adverse effect on the advertising function of the affected trademark (18). With respect to the function of indicating origin, the CJEU on the contrary imposed important obligations on advertisers to prevent consumer confusion :

« *In the case where the ad, while not suggesting the existence of an economic link, is* vague *to such an extent on the origin of the goods or services at issue that normally informed and reasonably attentive internet users are unable to determine, on the basis of the advertising link and the commercial message attached thereto, whether the advertiser is a third party vis-à-vis the proprietor of the trade mark or, on the contrary, economically linked to that proprietor, the conclusion must also be that there is an adverse effect on that function of the trade mark.* » (19)

The above has recently been confirmed by the CJEU in the Interflora/Marks & Spencer case (20).

As already stressed however, many uses of trademarks on SNS will probably not fall within the scope of « use in the course of trade » or « use in relation to goods or services », which are conditions precedent for a TM holder to invoke EU trademark legislation.

b. Art. 5(1)(b) CTMD and Art. 9(1)(b) CTMR.

In BergSpechte/Trekking.at the CJEU has also extended the above reasoning of the CJEU under art. 5(1)(a) CTMD and 9(1)(a) CMTR to Art. 5(1)(b) CTMD and Art. 9(1)(b) CTMR (21). Here of course, a likelihood of confusion must also be established.

c. Art. 5(2) CTMD and art. 9(1)(c) CTMR

Art. 5(2) CTMD and art. 9(1)(c) CTMR provide the holder of a reputed trademark with protection against dilution of their trademark. For such a TM holder to successfully invoke these articles they must establish the fulfilment of three additional conditions. Firstly, TM holders must show that their brand has a reputation (22). Secondly, they must establish at the very least a mere allusion to his trademark (23). Thirdly, TM holders must establish that the third party's use of an identical or similar sign (even in relation to goods or services which are not similar to those for which his trademark) takes unfair advantage of, or is detrimental to, the distinctive character or the repute of the trademark's reputation (24). The three modes of infringement are thus : detriment to the distinctive character (blurring), detriment to the repute (tarnishment) and unfair advantage from the distinctive character or repute (free-riding).

These thresholds for anti-dilution protection are counterbalanced by the flexible defence of "due cause" safeguarding comparative advertising (also applicable on art. 5(1)(a) CTMD or art. 9(1)(a) CTMR) (25) and parody (see further under 4) (26).

In the context of SNS mostly holders of reputed trademarks feel the need to protect their trademarks and can hence invoke the above articles to protect their trademarks against dilution. A TM holder can invoke blurring, for example when a third party uses a reputed trademark in connection with other goods or services (for example, a third party uses its postings to advertise luxurious Aston Martin clothing or jewellery ; the holder of the reputed trademark Aston Martin for automobiles does not want to permit such usage). Tarnishment shall occur for example when a third party associates a reputed trademark with substandard goods or services. This will result in damage to such trademark's reputation and in injury of its goodwill.

(iii) Territoriality

An additional problem for a TM holder seeking protection for his trademark on SNS (and the Internet in general) is that his trademark rights shall be limited territorially, depending on where the trademark has been registered. Neither global trademark protection nor injunction proceedings shall be available in the coming years, if ever. This shall therefore remain a permanent issue to be circumvented by TM holders.

(iv) Balance with freedom of expression

As we mentioned above the additional trademark protection against dilution may lead to endangering the fundamental freedom of expression.

Art. 5(2) CTMD and art. 9(1)(c) CTMR also comprise « due cause » safeguards for comparative advertising, parody and even more important, fundamental freedoms (for example, freedom of expression and freedom of competition).

With regards to comparative advertising the CJEU has already confirmed that the EU rules on comparative advertising can also be invoked with respect to art. 5(1)(a) CTMD and 9(1)(a) CMTR, meaning that a TM holder can only claim trademark infringement under those articles where such trademark was used by a third party for the purpose of comparative advertising without all the requirements in the Comparative Advertisement Directive being satisfied (27).

With regards to freedom of expression, the Internet will unavoidably oblige the

(16) See: C.J.E.U., 12 November 2002, C-206/01, *Arsenal/Reed*, para. 54; C.J.E.U., 18 June 2009, C-487/07, *L'Oréal/Bellure*, para. 60.
(17) C.J.E.U., 18 June 2009, C-487/07, *L'Oréal/Bellure*, para. 58.
(18) C.J.E.U., *ibid*., para. 98.
(19) C.J.E.U., *ibid*., para. 90.
(20) C.J.E.U., 22 September 2011, C-323/09, *Interflora/Marks & Spencer*, para. 45.
(21) C.J.E.U., 25 March 2010, case C-278/08, *BergSpechte/Trekking.at*, para. 36 and 39.
(22) See: C.J.E.U., 14 September 1999, case C-375/97, *General Motors vs. Yplon ("Chevy")*, para. 24-27.
(23) See: C.J.E.U., 23 October 2003, case C-408/01, *Adidas/Fitnessworld*, para. 29.
(24) See : C.J.E.U., 27 November 2008, case C-252/07, *Intel/CPM*, para. 77 ; the threshold has been lowered substantially in C.J.E.U., 18 June 2009, case C-487/07, *L'Oréal/Bellure*, para. 49.
(25) See : C.J.E.U., 18 June 2009, case C-487/07, *L'Oréal/Bellure*, para. 54 and 65.
(26) M. Sentfleben, *Adapting EU trademark law to new technologies – back to basics ?*, p. 13, available at www.ssrn.com/abstract=187569.
(27) See : C.J.E.U., 18 June 2009, case C-487/07, *L'Oréal/Bellure*, para. 54 and 65.

CJEU to reconsider the balance between trademark protection and fundamental freedoms. The keyword advertisement cases before the CJEU seem to have triggered this debate (28). In the Google cases, the AG decided Google did not use the trademark in the sense of trademark laws. Keyword advertising services have been placed beyond the control of the TM holder. In the Interflora/Marks & Spencer case for example, the use on Google's advertising services by M&S of an identical sign (Interflora) to the trade mark (INTERFLORA) in relation to identical services, namely flower-delivery services, was at issue. AG Jääskinen proposed to focus on the fairness of the use instead of simply looking at the advantage someone takes of the repute of a reputed trademark stating that the mere reference to a trademark is not necessarily a use within the meaning of trademark laws (29).

At present it remains an open question as to how the CJEU will further deal with such questions about the balance between trademark rights and fundamental rights.

C. Conclusion on trademarks

Traditional enforcement has proven to be outdated and ineffective when speaking about IP protected content on SNS. Even though it might be possible in certain cases to resort to traditional IP legislation, prevention and soft repression are the keywords for successful IP management in a social media environment.

To prevent the threats of social media to their trademarks, TM holders should register their trademark or username and identify interesting sub-domain names. They should create their own pages or fan sites on SNS. TM holders should monitor the use of their trademarks on SNS. TM holders should also on a regular basis launch marketing campaigns in order to educate the public about the ownership of their trademark. Finally, TM holders should keep a record of all action taken to ensure demonstration of proper control of the trademark should it ever be useful or required in the future.

III Copyrights on social media

A. General copyright rules

The general copyright rules also apply to SNS given the technological neutral character of our Belgian Copyright Act.

An owner of copyright protected social media content shall thus have the right to prevent third parties amongst others from reproducing or communicating such content to the public. But when is content on a SNS copyright protected ?

Copyright protection is granted to content which is original and which has been expressed in a concrete form.

The latter condition shall not pose many problems. In many cases the holder of social media content will therefore only need to establish that the content reaches the necessary level of originality. Are Facebook-uploads or Tweets original ? That is the question.

With its 140 character limit one would think that a Tweet will hardly ever reach the level of originality required for copyright protection. It must be stressed however that the length or size of a work does not play any role in obtaining copyright protection (30). There is no doubt that an original newspaper heading is copyright protected. Similarly, a Haiku (a short Japanese poem) can be copyright protected. Hence, we believe there is no reason to exclude Tweets from copyright protection. But there is another problem. Facts are not copyrightable and aren't facts what Tweets are about ? Tweets are mostly about facts but not always.

B. Exceptions

Also, the exceptions to copyright rules shall apply to SNS. Hence, a third party can invoke the copyright exceptions of quoting and parody to circumvent copyright protection for social media content and can reproduce or communicate an original work to the public without authorisation of the copy holder. The above exceptions are of course subject to the usual conditions.

Quoting is only allowed under the Belgian Copyright Act for purposes of criticism, controversy, or education, in the framework of scientific works, or for review (31). Free quoting is not allowed for other purposes.

The Belgian Copyright Act also provides an exception for the « *use for the purpose of caricature, parody or pastiche* ». This exception applies even when all the essential elements of the original work have been copied.

A parody may however never affect the honour and reputation of the original author or mutilate his work. The limits of humour, mockery or even decency cannot be exceeded, not even on SNS (32).

C. The threats

One needs to distinguish on the one hand the content published by companies or their employees and on the other hand the content published by others, being user generated content.

Companies considering their own content should first address the copyright ownership issue. Indeed, the original content copyright owner will often be an employee and hence will be the original copyright holder. Companies can obtain copyrights by transfer or licence in a written agreement or labour contract in which such licence or transfer needs to be circumscribed explicitly (33).

Furthermore, companies should keep track of their copyright protected content. A simple watermark on a photo could give certainty about the origin of the

(28) See : *AG Poiares Maduro*, opinion of 22 September 2009, cases c-236/08-238/08, *Google France and Google/Louis Vuitton et al.*, para. 102 ; *AG N. Jääskinen*, opinion of 9 December 2010, case c-324/09, *L'Oréal/eBay*, para. 49 ; *AG N. Jääskinen*, opinion of 24 March 2011, case C-323/09, *Interflora/Marks & Spencer*, para. 94.

(29) *AG Jääskinen*, opinion of 24 March 2011, case c-323/09, *Interflora/Marsk&Spencer*, para. 96-106.

(30) See for example: Tribunal of First Instance Brussels, 13 February 2007, *A&M* 1/2007, 107, with note D. Voorhoof, « Slecht nieuws voor Google News » , 12 0 : « *Attendu que si tous les titres d'articles de journaux ne peuvent être considérés comme originaux – certains paraissant effectivement purement descriptif et ne révélant, dès lors, pas l'empreinte de leur auteur – il ne peut toutefois être estimé qu'aucun titre d'articles de presse ne présenterait une originalité suffisante pour pouvoir bénéficier de la protection de la loi sur le droit d'auteur* » .

(31) In this respect GoogleNews could not invoke the right to quote: Tribunal of Brussels, 13 February 2007, *A&M*, 2007, 107, with note D. Voorhoof.

(32) Brussels 8 June 1978, *J.T.*, 1978, 619 ; Antwerp 11 October 2000, *I.R.D.I.*, 2001, 137, *A&M*, 2001, 357, note D. Voorhoof.

(33) See for example: Brussels 28 October 1997, *I.R.D.I.*, 1998, 44, note. M.C. Janssens.

photo. Copyright information that goes with the content (such as the name of the company and the mention of « copyrights reserved ») may serve the purpose of protecting the company's content.

When copyright protected content has on the contrary been put on-line by a third party, the rules of user generated content shall apply. In many cases it will be difficult to establish the identity of the third party. SNS can invoke the limited liability principles of mere conduit, caching and hosting under the E-commerce Directive (34).

As for trademarks copyright infringements can be dealt with preventatively or repressively. All preventative measures are preferable. Overreaction is to be avoided. In general even if repression is the only solution soft repression is to be preferred over hard repression which may lead to an even worse situation than before (for example, The Barbara Streisand effect: she sued Pictopia.com in 2003 for aerial photo's put on the website and within a week the page had 420,000 hits). Most SNS have policies which make it possible to notify of infringements of intellectual property rights.

D. Conclusion on copyrights

Before posting copyright protected content on social media, companies should be well aware that they might lose control of such content through their employees amongst others. Informing and educating these employees can prevent such loss of control.

With regards to repression, most SNC offer tools for copyright owners to address copyright infringements. In many cases those tools should suffice and addressing claims to traditional courts should thus be the last step to consider.

IV Data protection and Privacy (35)

Not only intellectual property rights and consumer protection rights are to be taken into account when a company is active on SNS and, more broadly, on the internet. Data protection and privacy regulations apply as well and have far-reaching implications.

A company active on SNS will most probably process personal data, which entails specific obligations imposed by data protection law. This will be addressed in section A below.

Further, the company may wish to monitor the online behaviour of its employees on SNS in relation to the company, which is subject to privacy restrictions. This will be addressed in section B below.

A. Data Protection Obligations

Most companies today are aware of the advantages of being present on SNS. It is the perfect place to interact with customers and add an online dimension to the company's identity.

However, most companies are not sufficiently aware of the obligations that such a virtual identity brings about. A number of these obligations originate in data protection law. In Belgium, the relevant law is the Act of 8 December 1992 on the protection of privacy in relation to the processing of personal data (« Privacy Act ») (36).

1. *Data controller and data processor*

The Privacy Act defines who is the controller of the data processing, and who is the processor. The *controller* is the party who determines the purpose and means of the processing (37). The *processor* processes personal data on behalf of the controller (38).

The distinction between data controller and data processor is intended as a means of allocating responsibility. The bulk of the obligations rest on the data controller : he is responsible for ensuring that the data is processed lawfully. Pursuant to Opinion 1/2010 of the Article 29 Data Protection Working Party on the concepts of « controller » and « processor » (39), the essential obligation of the data controller is to determine who shall be responsible for compliance with data protection rules, and how data subjects can exercise their rights in practice. The concept of « controller » is autonomous in that it should be interpreted mainly in accordance with European Community data protection law. It is a functional concept, in the sense that it is intended to allocate responsibilities where the factual influence lies. The concept of « controller » is thus based on a factual rather than a formal analysis.

The Article 29 Working Party considers that the party who determines the *purpose* of the data processing will always trigger the qualification as data controller. Conversely, the party who determines the means of the processing will only trigger such qualification if these means are essential, rather than merely technical and organisational (40).

The identity and location of the data controller determines the applicable law in case of cross-border data transfers. The Belgian Privacy Act applies (i) to the processing of personal data within the framework of activities that take place in Belgium and (ii) to the processing of personal data by a controller who is not permanently established on European Community territory, if the means used (automated or not) are located on Belgian territory and are not used for the sole purpose of transit of personal data over Belgian territory (41). In scenario (ii), the data controller is required to nominate a representative on Belgian territory.

The data processor acts under the instructions of the controller and therefore has a more limited responsibility. However, the concept of processor plays an important role in the context of confidentiality and security of processing. Since the data processor is more closely involved with the factual processing of the data, he is jointly responsible with the data controller for the security of such processing. The identity and location of the processor also have an impact on the applicable law. Pursuant to Directive 95/46/EC, the Belgian Privacy Act applies to the security of the data processing if the data processor is located in Belgium (42).

(34) Article 12, 13 and 14 of Directive 2000/31/EC on electronic commerce.

(35) Written by Patricia Cappuyns with the collaboration of Matthias Vierstraete.

(36) *Belgian State Gazette*, 18 March 1993, as amended.

(37) Article 1 §4 of the Privacy Act.

(38) Article 1 §5 of the Privacy Act.

(39) Available online at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf. The Article 29 Working Party is an independent European advisory body on data protection and privacy, set up under Article 29 of Directive 95/46/EC. It includes representatives of the various privacy bodies of the European Member States.

(40) Opinion 1/2010, cited above, p. 14. See also E. Verbrugge, « Verwerking van persoonsgegevens », in P. Van Eecke, *Recht & elektronische handel*, Larcier, Gent, (232), 239.

(41) Article 3*bis* Privacy Act. The « means used » are interpreted very broadly. If the SNS uses cookies or JavaScripts to process the personal data of a SNS user whose computer is located in Belgium, then such processing will be subject to the Privacy Act. See E. Verbrugge, « Verwerking van persoonsgegevens », in P. Van Eecke, *Recht & elektronische handel*, Larcier, Gent, (232), 243.

(42) Article 17(3) Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the « Data Protection Directive »). The European data protection regime is currently under review.

2. *Who is who in social media?*

We would argue that the distinction between data controller and data processor is no longer suited to Web 2.0 generally and SNS in particular. It is very difficult, if not impossible, to clearly delineate who determines the purpose and means of the data processing: the SNS or the company who uses it as an on-line platform. While the Article 29 Working Party recognises the fast-moving evolution of the internet and the considerable age of the Data Protection Directive, it concluded that *« it has not found any reason to think that the current distinction between controllers and processors would no longer be relevant and workable »* in a complex online environment (43). We respectfully disagree. Still, until such time as legislative modifications are introduced to fine-tune these concepts and the resulting division of responsibility, we will have to make do with the legislative and interpretative tools we currently have. These are discussed below.

Opinion 5/2009 of the Article 29 Working Party on social networking (44) considers that the SNS providers are data controllers, since they determine the purpose and the means of the processing (45). The users of the SNS – including companies – may qualify as joint data controllers if their actions are not subject to any data protection exemptions (46).

Consider the case where a company makes available on its SNS-profile pictures of a corporate function, or a video in which employees are shown at work or in which they present the services of the company. In such cases, the company determines the purpose of the data processing, namely the positioning of the company and its brand in an online environment. In addition, the company determines the means through which the data are made available online: the SNS-profile to be used, the duration of the availability and so on. Therefore the company is the joint controller of the personal data (such as pictures, videos, and names) that are made available online and it shares data controller responsibilities with the SNS. In most cases, such companies do not fall under any of the exemptions provided in the Privacy Act (47). This means that they will be jointly responsible with the provider of the SNS to ensure that data protection obligations are complied with. Unfortunately, the Article 29 Working Party does not address the practical consequences of such joint liability (48). In what follows, we will examine how companies can ensure that they comply with their obligations as joint data controllers.

3. *What companies with SNS profiles should do*

Companies who use SNS should not assume that the SNS provider is doing enough to ensure compliance. For starters, such companies should check with the SNS provider whether they have filed a notification with the Belgian Privacy Commission prior to the data processing (49). In addition, companies are advised to inform individuals acting under their authority of the provisions of the Privacy Act and other relevant provisions, and to take internal measures to ensure compliance with their data protection obligations (50). Also, companies are advised to inform data subjects directly through their SNS profile about the purpose of the data processing, the recipients of the data, the data subjects' right to object to the processing and to access and rectify the data processed (51).

Many companies do not provide such information on their SNS-profile and may as a result be in violation of their data protection obligations. An easy solution is to provide such information in a privacy policy, which is made available either directly on the SNS company profile or through a link to the official website of the company. Importantly, such a reference to the privacy policy cannot be equated to the acceptance of the policy by the data subject, i.e. « consent » in data protection terminology. Consent is required because it is the main legal basis for lawful data processing (52). The data subject's consent can be obtained by providing a pop-up box to be ticked to indicate acceptance of the policy.

If the data subject is a third party and not a visitor of the company's SNS profile (e.g. an individual who is identifiable on a picture posted by a visitor of the SNS profile), it will not be possible for the company to obtain the third party's consent. Therefore, the company's privacy policy should include a warning to users that visitors of the company's SNS profile should not provide personal data about third parties without their consent.

4. *Conclusion on data protection*

Is this all new ? No. The Privacy Act has applied for some time in the offline world. However, as more and more companies create SNS profiles and use them in ever expanding ways, they should become more astute to the legal implications and the risks involved. Data controllers can currently be fined up to 550,000 EUR, and in certain limited cases there is the possibility of imprisonment if they do not comply with their data protection obligations. Good communication with and monitoring of the SNS provider is key, as is the need for a well-written privacy policy.

B. Your Brand in the Hands of Employees: Cyber Surveillance

Employees have access to SNS during and also after working hours, whether it is through computers at the office, at home or via mobile devices. What employees say about or on behalf of their company may have far-reaching consequences. There are plenty of examples of employees who have created embarrassment or liability for their employers through their activities on SNS (53).

(43) Working Party 29 Opinion 5/2009 of 12 June 2009 on online social networking, available at http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2009_en.htm, p. 33.
(44) Working Party 29 Opinion 5/2009, cited above.
(45) See also Opinion 1/2010, cited above, Example No 12 on p. 21.
(46) Such as the household exemption, the exemption for journalistic purposes, for artistic or literary expression; see Article 3 of the Privacy Act. Most companies will not fall under any of these exemptions.
(47) The Article 29 Working Party refers to the household exemption as an easy way out of data controller obligations. However, this exemption will generally not apply to companies, so it doesn't absolve companies with SNS profiles from their data protection obligations.
(48) See for a critical analysis of the Article 29 Working Party Opinion on this point: Prof. Dr. P. Van Eecke and Mr. M. Truyens, « Privacy en sociale netwerken » in *Computerrecht*, 3/2010, (115), 121 and 123. We also refer to the advice and the decision of the Belgian Privacy Commission in the SWIFT case, which concerned the qualification as joint data controllers in a different context. The advice is available online at http://www.privacycommission.be/nl/docs/Commission/2006/advies_37_2006.pdf[; the decision is available at http://www.privacycommission.be/nl/static/pdf/cbpl-documents/swift---nl-final-09.pdf.
(49) Article 17 Privacy Act.
(50) Article 16 § 2 Privacy Act.
(51) Article 9 of the Privacy Act.
(52) Article 5 a) of the Privacy Act.
(53) For a few examples, see http://www.independent.co.uk/news/uk/home-news/virgin-atlantic-sacks-13-staff-for-calling-its-flyers-chavs-982192.html (Virgin Atlantic) and http://www.dailymail.co.uk/news/arti-

Their statements may have an impact on the company's reputation, they may give rise to the company's liability for unlawful acts (54), they may lead to the disclosure of confidential information, to security breaches and to non-compliance with data protection law. In addition, employees' activities on SNS may lead to a huge waste of time and resources.

It is clear that it may be worthwhile for companies to monitor their employees' activities online so that they can take action (including dismissal) if employees overstep the boundaries. The question arises how far companies can go in such « cyber-surveillance ». Employees will probably oppose surveillance on the basis of their right to private life and correspondence (55), rights that are – to a more limited extent – also protected in the workplace (56). However, these rights are not absolute and it is possible for employers to encroach upon them in certain cases (57). For a good overview of the applicable law and the balance that has been struck by the Belgian legislator, we refer to the Report on cyber-surveillance of July 2011 of the Belgian Privacy Commission (58).

1. *The principle of secrecy of telecommunications*

Article 124 of the Act on Electronic Communications (59) (AEC) and article 314*bis* of the Belgian Criminal Code establish the principle of the secrecy of electronic communications. The secrecy of electronic communications is twofold. On the one hand, it is prohibited to take cognisance of the *content* of the communication during the transfer thereof (article 314*bis* of the Criminal Code). On the other hand it is prohibited to take cognisance of the *existence* of the communication, not only during the transfer thereof but at any time (Article 124 of the AEC).

In a recent judgment, the Hof van Cassatie/Cour de Cassation held with respect to Article 124 AEC that taking cognisance of and using the *content* of an e-mail is connected to taking cognisance of and using the *existence* of the communication (60). The Privacy Commission considers that this holding may support the conclusion that Article 124 AEC not only protects the secrecy of the *existence* of the communication, but also the secrecy of its *content* (61). This may mean that, without consent, an employer is not allowed to intentionally scan the inbox of his employees and use the content of an offending e-mail against them, even for the purpose of an urgent dismissal. It must be said however that this interpretation of the Privacy Commission is disputed, one of the reasons being that the judgment of the Hof van Cassatie/Cour de Cassation did not arise in an employment context.

2. *Exceptions to the secrecy of telecommunications*

So it looks like the possibilities for an employer to lawfully monitor its employees' internet use are quite limited. Of course, some common sense exceptions apply.

Firstly, there is in theory no violation of these articles if the employer obtained the consent of all the participants in the electronic communication. To monitor the activities of employees on SNS, it may be sufficient to obtain the employees' consent in a labour regulation, in the employment contract or in the company's e-mail and internet policy. However, the question arises whether any « consent » given by an employee in an employment relationship, which by definition entails an element of subordination, can be considered to have been given freely (62). Relying solely on a contractual consent of the employees is therefore somewhat risky.

Secondly, article 125, 2° AEC states that the above prohibitions do not apply if the only purpose of the monitoring is to verify the performance of the network and to guarantee the performance of the electronic communication service.

Thirdly, article 128 AEC allows *inter alia* the keeping of a record of electronic communications in order to prove a commercial transaction or any other business communication. However, it is still necessary to inform the concerned parties before such a recording that it will take place, what the purpose of the recording is and how long the recording will be kept. This exception does not allow employers to generally monitor the e-mail and internet use of their employees.

Fourthly, article 125, 1° AEC states that article 124 AEC is not infringed in cases where the activities concerned are allowed or made obligatory by law. A number of articles in the Act on Labour Agreements of 3 July 1978 may serve as a legal basis for the monitoring of employees' internet use, in particular the articles that concern the right of the employer to exert authority over his employees (63). Belgian courts have accepted these articles as a sufficient legal basis for the employers' right to monitor employees' internet and e-mail use (64).

On this basis, some practical guidelines regarding the employer's right to cyber-surveillance have been worked out in Collective Labour Agreement Nr. 81 of 2002 (65). This CLA does not take precedence over the statutory provisions mentioned, but it does provide a good framework for companies that want to engage in cyber-surveillance without violating their employees' right to privacy.

3. *Use of unlawfully obtained evidence*

The question is whether evidence obtained through cyber-surveillance may be used against employees, for example to justify their dismissal, if it was obtained by the employer in violation of the applicable law (e.g. the Criminal Code, the AEC, CLA 81 or the Privacy Act). One would expect that an employee who is dismissed based on information that the employer obtained in violation of the applicable law on cyber-surveillance, can successfully challenge this dismissal on this basis.

cle-1082437/BA-check-staff-post-comments-smelly-passengers-Facebook.html (British Airways).

(54) Article 1384 of the Belgian Civil Code.

(55) Article 8 § 1 of the European Convention on Human Rights.

(56) ECHR, *Copland vs. United Kingdom*, 3 April 2007, paragraph 41 and 42, and the cases referred to therein (http://www.echr.coe.int).

(57) Article 8 §2 of the European Convention on Human Rights.

(58) Available at http://www.privacycommission.be/nl/static/pdf/cyber-surveillance/juridisch-rapport.pdf. A new report on cyber-surveillance is expected from the Belgian Privacy Commission in the beginning of 2012, which will detail its findings after a public consultation on the subject.

(59) Act on Electronic Communications of 13 June 2005, *Belgian State Gazette*, 20 June 2005.

(60) Cass., 1 October 2009, docket number C.08.0064.N, § 4, available at www.juridat.be.

(61) See the report of the Belgian Privacy Commission of July 2011, p. 9.

(62) See the report of the Belgian Privacy Commission of July 2011, p. 10.

(63) In particular Articles 2, 3, 4, 5, 16 and 17.

(64) See for some examples the case-law cited in the report of the Belgian Privacy Commission of July 2011, p. 12. It goes without saying that, when an employer monitors his employees' internet use, he must still comply with any data protection obligations he is subject to.

(65) CAO 81 on the protection of the private life of employees in relation to the control on electronic online communications (2002), available at http://www.cnt-nar.be.

However, in the Antigoon case, the Hof van Cassatie/Cour de Cassation limited the conditions under which unlawfully obtained evidence can be refused in the context of a criminal investigation (66). The Court ruled that evidence obtained unlawfully can only be refused in three circumstances : (i) violation of a formal requirement on pain of nullity, (ii) the illegality has undermined the reliability of the evidence or (iii) the use of such evidence is in violation of the right to a fair trial. While the Antigoon case concerned a criminal investigation, the Court held in 2008 that the same principles apply in a labour context, and the lower courts have in a number of cases followed this approach (67).

4. *Conclusion on privacy*

Companies that wish to monitor their employees' activities on SNS are advised to inform their employees that their internet use will be monitored, and to obtain their consent to such monitoring. Further, companies should follow the principles and guidelines set forth in CLA 81. Finally, even if the evidence for a dismissal was seemingly obtained in violation of the applicable law on cyber-surveillance, it may still be effective against the dismissed employee in subsequent court proceedings in light of the Antigoon case law of the Hof van Cassatie / Cour de Cassation.

Iain Stansfield,
Christine De Keersmaeker
Patricia Cappuyns
Avocats

(66) Cass., 14 October 2003, docket number P.03.0762.N, available on www.juridat.be.

(67) See the case law mentioned in the report of the Privacy Commission of July 2011, p. 25.