ECTA
European Communities Trade Mark Association

32nd ANNUAL CONFERENCE

THE JURY IS STILL OUT

BUCHAREST, 19-22 June 2013
Social platforms

Data protection and IP rights on social platforms
Social platforms - Data protection and IP rights on social platforms

Questions & Answers

Katja Grabienski
Attorney-at-Law
Chair of the ECTA Publications Committee

Dr. Peter Schramm
Attorney-at-Law
Member of the ECTA Design Committee
Social platforms - Data protection and IP rights on social platforms

I. Introduction

Different types of social media:

• collaborative projects (Wikipedia, etc.)
• blogs (Twitter, etc.)
• content communities (Youtube, MyVideo etc.)
• social networking sites (Facebook, Xing, Linkedin, etc.)
• virtual games worlds (World of Warcraft, etc.)
• and virtual social worlds (Second Life etc.)
Social platforms - *Data protection and IP rights on social platforms*

I. Introduction

Legal Vacuum?
Social platforms - *Data protection and IP rights on social platforms*

I. Introduction

Legal issues:

- Data protection
- IP Infringements
Social platforms - Data protection and IP rights on social platforms

II. Data Protection
II. Data Protection

Social media monitoring:

- Is this service permissible under applicable law from a data protection perspective?
- Is my company allowed to use the data for my marketing activities?
YES, BUT

- Data protection laws will in many countries allow monitoring only.
- Some suppliers of respective web tools require compliance with certain minimum data protection criteria. For instance, if you use Google Analytics for Germany, you will have to comply with five requirements set by Google. Google has negotiated these points with German data protection authorities in 2011. Similar contractual restriction may apply from time to time also with Facebook’s company account analysing tools, etc.
II. Data Protection

So-called “Cookies”

Without cookies, you can only monitor the IP address visiting your website. The IP address is in most cases dynamic, i.e. next time the person clicks on your website, it will be a different IP address.

With cookies, you can identify the “person”. At least, you can monitor that the same user is entering the website and monitor and analyse his clicks.
II. Data Protection

Use of Cookies:

May companies use cookies to get “user-input” in order to engage into marketing research, communication, sales promotions/discounts, and relationship development/loyalty programs?
II. Data Protection

Article 5.3 of e-privacy Directive (Directive 2002/58/EC, as amended by the “Cookie-Directive” 2009/136/EC) allows cookies to be exempted from the requirement of informed consent, if they satisfy one of the following criteria:

- The cookie is used "for the sole purpose of carrying out the transmission of a communication over an electronic communications network";

- The cookie is "strictly necessary in order for the provider of an information society service requested by the subscriber or user to provide the service".
No “user-input cookies” without user’s content, but the directive leaves the following questions open:

• Must the internet-user give its consent to the cookie to be implemented on its computer (“opt-in”), or

• are the setup parameters of the user's Internet browser sufficient to comply with the law (“opt-out”)?
Social platforms - *Data protection and IP rights on social platforms*

II. Data Protection

*Use of Cookies:*

*How is the situation in the European countries?*
II. Data Protection

Different legal situation in the European countries:

- “Opt-in countries”: Denmark, France, UK, Netherlands, Spain, Sweden, Switzerland
- “Opt-out countries”: Bulgaria, Finland, Luxemburg, Slovakia, Czech republic
- Unclear: Rumania, Germany, Greece, Italy etc.
II. Data Protection

Use of Cookies:

To be on the safe side: How can I comply with the “Opt-in” requirement?
Legally permitted ways to use cookies:

- **Information banner** on the top of a website requesting the user's consent to set some cookies, with a hyperlink to a privacy statement;
- A **splash screen** on entering the website explaining what cookies will be set by what parties if the user consents;
- A **tick box** at the time of the registration to an online service.
II. Data Protection

Social Media Marketing:

May a company use the information/data obtained by social media monitoring in order to engage into marketing research, communication, sales promotions, loyalty programs, etc.?
Article 5.1 of Unfair Commercial Practices Directive (Directive 2005/29/EC) forbid any unfair commercial practices, Article 5.5 refers to Annex I which contains the list of those commercial practices which shall in all circumstances be regarded as unfair.

#26 of this “Black List”:

Making persistent and unwanted solicitations by telephone, fax, e-mail or other remote media except in circumstances and to the extent justified under national law to enforce a contractual obligation.
You can analyse the data. **But** you will need an expressed consent from a consumer before sending custom-tailored communication of any kind... **unless** you act in the frame of an existing contract with that customer.

**Two open questions:**

- What exactly is expressed consent and how can it be proven.
- What is in the frame of an existing contract, only the existing contract or similar/extending contracts and offers?
III. IP infringements on social platforms
General filtering systems:

Are the social network providers obliged to install **general filtering systems** for the prevention of copyright infringements?
ECJ C-360/10 – Sabam vs. Netlog

- **E-Commerce Directive**: Member States are not allowed to impose a general obligation to monitor on service providers conducting activities of mere conduit, caching and hosting;
- **General filtering systems** challenge several fundamental rights, such as the freedom to conduct a business or customer data protection and the freedom of information (as the system might not have been always able to distinguish between unlawful content and lawful content, eventually blocking lawful communications);
- **Copyright protection** may vary from one Member State to another; in some Member States certain works fall within the public domain or may be posted online free of charge by the authors concerned.

➤ **Social network providers cannot be obliged to monitor, filter and block alleged infringing content.**
IP infringements:
We heard about some means called “notice-and-take-down” or NTD.
What is that?
Social platforms - Data protection and IP rights on social platforms

III. IP infringements on social platforms

“Notice-and-take-down” (NTD)

• Legal complaint system in the USA

• Section 512 c U.S. Copyright Act: “upon notification of claimed infringement” the Internet Service Provider (ISP) should respond “expeditiously to remove, or disable access to the material that is claimed to be infringing or to be the subject of infringing activity”.
Social platforms - Data protection and IP rights on social platforms

III. IP infringements on social platforms

Mandatory information for NTD complaint:

• name of the owner of an exclusive right (or an authorized person),
• identification of the copyrighted work claimed to have been infringed,
• identification of the material claimed to be infringing,
• contact information of the complaining party,
• statement of good faith of the consignor that the use of the material is not authorized, statement that the information is accurate.
III. IP infringements on social platforms

“Safe Harbour”:

- No liability as long as the ISP/social network provider takes down the infringing material immediately after receipt of a NTD complaint, it will not be liable for any infringement.

- If the ISP has actual knowledge of an obviously illegal content, he has to act without waiting for a notification in order not to lose its “safe harbour”.
Social platforms - Data protection and IP rights on social platforms

III. IP infringements on social platforms

“Safe harbour” in the EU:

May the social network providers also rely on a “safe harbour” system in the EU?
III. IP infringements on social platforms

Articles 12-15 of the e-Commerce Directive (2000/31/EC)

- **“mere conduit defense”** - ISP neither initiates the transmission, selects the receiver of the transmission nor selects or modifies the information contained in the transmission = “safe harbour”, no liability

- **“hosting defense”** – storage of use (generated) content = “safe harbour” if the ISP does not have actual knowledge of infringement or obvious facts and expeditiously removes or disables access to such content upon obtaining such knowledge.
Social platforms - Data protection and IP rights on social platforms

III. IP infringements on social platforms

**German Federal Court of Justice (BGH - decision of 25.10.2011, VI ZR 93/10 – Blogspot):**

- Blog provider liable as secondary infringer („Störerhaftung“)

- If the impaired party produces supporting documents, the host provider has to make its own inquiries about the possible infringement to enter into a “safe harbor”.
Social platforms - Data protection and IP rights on social platforms

III. IP infringements on social platforms

- District Court Nürnberg-Führt (8.5.2012, 11 O 2608/12) and recently Berlin’s Appeal Court (7.3.2013, 10 U 97/12) confirmed these requirements.

- For instance, YouTube and Facebook have respective online contact opportunities for filing such notices.
Social platforms - *Data protection and IP rights on social platforms*

III. IP infringements on social platforms

**Framing:**

May the making of a movie publicly accessible through a website by ‘framing’ this content from a content community like Youtube be qualified as copyright infringement after the laws of the EU member states?
III. IP infringements on social platforms

Main question:

Does framing constitute a copyright infringing “making available to the public” in the sense of Article 3(1) of Directive 2001/29/EC?
Social platforms - Data protection and IP rights on social platforms

III. IP infringements on social platforms

Request for Preliminary ruling by the German Federal Court of Justice (BGH, 16.05.2013 - I ZR 46/12):

• BGH: the mere linking of content that is provided on a separate website by ‘framing’ this content does not constitute ‘making available to the public’ within the meaning of German copyright law;

• However, the BGH wondered whether framing could fall under Article 3(1) of Directive 2001/29/EC asked the ECJ whether framing is a “making available to the public” in the sense of Article 3(1) of Directive 2001/29/EC.

• If so, this would also be an infringement of German copyright law and probably also after the copyright laws of all further EU-member states.
Social platforms - *Data protection and IP rights on social platforms*

III. IP infringements on social platforms

**Framing:**

*What are the consequences?*
Legal situation in the EU unclear:

- Website owner should check if he is allowed to use the “framed” content on his website, above all on commercial websites.
- If not, the website owner should work with “hyperlinks”, i.e. make clear that the foreignness of the content is clearly visible.
Thank you!