

Amica project

High level analysis legal issues

Patrick Van Eecke



Our understanding of the project

- Web 2.0 (blogs, chat rooms, social networks)
 - Risks associated with use of Web 2.0 for illegal or malicious purposes, specifically in relation to the development of minors
- Amica
 - Automatic monitoring procedure which can process data overload in an intelligent way
 - Process which sends alerts in critical situations and which aims to reduce the illegal and abuse use of SNS
 - The methodology is also applicable for other applications (e.g. e-health). [This analysis does not yet take into account such other applications in this phase of the project.]

Legal perspective³

the right balance between

privacy
freedom of speech

prevention
enforcement

Legal perspective

the right balance between

privacy
freedom of speech

prevention
enforcement

from the perspective of:

- end user victim (child, employee, ...)
- end user offender (child, adult, employee, employer, school, ...)
- controlling party (parent, employer, ...)
- legal/administrative authority (CCU, Child focus, ...)

Legal questions raised by⁵ Amica

- Privacy issues
- However, other legal issues arise as well: level of intervention *allowed*, criminal law, freedom of speech, international aspects, etc.
- No analysis from an ethical or social perspective, only a high level overview of legal issues.
- Analysis under Belgian law



Methodology

Universiteit Antwerpen



Methodology

- For each use case, it will need to be examined (in addition to the ethical and social acceptability of each use case)
 - what is the exact legal qualification of the monitored behaviour, and the consequences thereof;
 - whether and how the requirements of the Data Protection Act can be complied with;
 - which specific legislation applies to the use case;
 - which are the liability risks in case Amica is defective.

General analysis of the project



1. Information concerned

- *Personal data*
 - In general: e.g. screen name, blog posts
 - Sensitive data: e.g. medical (mental) data in case of self-mutilation, racial information (photos)
 - Criminal data: e.g. actions of a paedophile
 - IP addresses?
- *Different types of content*
 - Text
 - Photos and video footage

1. Information concerned

- *Information without (sufficient) context*
 - E.g. an isolated reaction to a blog post which appears harmful, but is in fact to be seen in the context of an "inside joke" between adolescents
 - E.g. a naked picture of a young girl who looks 14, yet is 20 years old

2. Parties involved

- *Actors involved in harmful content*
 - Originator: e.g. a paedophile grooming the Internet; a bully sending harmful messages via Netlog; a young girl sending naked pictures to her boyfriend via Facebook; a person creating a blog regarding islamist ideas
 - Recipient: e.g. a child being groomed or bullied; a child being confronted with advertisements for escort services on a social network; a person receiving racist messages via Facebook
 - [Other?]

2. Parties involved

- *Actors involved in use of Amica*
 - Amica itself: provides a product/service
 - "Buyer"/"user": e.g. parents purchasing monitoring software, an employer purchasing monitoring software, a social network site implementing the software
- Third party stakeholders: e.g. police and the authorities in case of criminal conduct, suicide prevention hotline

3. The product

- Is Amica "customisable"?
 - Can parents for example request that only they are warned in case of suicidal inclinations of their child, and not the police or suicide hotline?
 - Can Amica distinguish between minor, important and severe issues? Can a "user" request Amica to be installed so that it only picks up "severe" issues?

General overview applicable legislation



Legal issues

- Data protection
- Secrecy of communication
- Liability
- International aspects

Treaty on the European Union

- Title I - Common Provisions - Article 6
 - The Union is founded on the principles of liberty, democracy, respect for human rights and fundamental freedoms, and the rule of law, principles which are common to the Member States.
 - The Union shall respect fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms signed in Rome on 4 November 1950 and as they result from the constitutional traditions common to the Member States, as general principles of Community law.
 - The Union shall respect the national identities of its Member States.
 - The Union shall provide itself with the means necessary to attain its objectives and carry through its policies

European Convention for the Protection of Human Rights and Fundamental Freedoms

17

- Article 8
 - Everyone has the right to respect for his private and family life, his home and his correspondence.
 - There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.



Data Protection Directive¹⁸

- Official name
 - Directive 95/46/EC of the European Parliament and of the Council 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
- Regulates:
 - the manner in which personal data can be gathered in the EU;
 - the rights of EU citizens with respect to their personal data;
 - the transfer of personal data to non-EU countries.
- Principles
 - Notice
 - Choice
 - Onward Transfer
 - Access
 - Security
 - Integrity
 - Enforcement



When does the law apply?¹⁹

- **Processing**

- collection, recording, organisation, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment, combination as well as blocking, erasure or destruction of personal data

When does the law apply?

20

- **Personal data**

- = any information relating to an identified or identifiable natural person
- an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity
- E.g. (name, adress, phone numer, ...)

Data Protection Act

- Distinction to be made between "controller" and "processor"
 - Relationship between parties can be regulated via contractual arrangements to a certain extent
 - However, factual circumstances are decisive: it will need to be examined to which extent Amica could be considered a controller

- Any processing of personal data requires a legal basis
 - The most relevant in this context are:
 - Consent
 - Vital interest of the data subject
 - Legitimate interests of the controller
 - This also heavily depends on which party is deemed controller. For example, use of Amica by the FCCU could be argued to be necessary for the execution of a task of public interest.
- The controller has an information obligation towards the data subject
 - Difficult to comply with vis-à-vis "Senders" and "Recipients"

Secrecy of communication

- *Article 314bis Penal Code*
 - Prohibits the interception of telecommunication
- *Article 124 Telecom Act*
 - Protects the secret of electronic communications: one cannot gain knowledge of any electronic communications without the consent of all parties involved in the communication
 - Very broadly described (yet subject to discussion)
- Often not only deemed to relate to communications between persons, but also communication between a person and a "machine" (e.g. Internet traffic)

Liability

- Guarantees of functionality?
- Contractual liability vis-à-vis "Buyer"
- Exclusions of liability vis-à-vis consumers (e.g. parents)? Possibility to exclude liability for death / bodily injury?
- Extra-contractual liability: can Amica be held liable extra-contractually, e.g. in case of a wrongful intervention causing reputational damage to an alleged paedophile?
- Criminal liability: can lack of sufficient intervention constitute an offence of "criminal omission"?

International aspects

- How will this Amica be used in an international online context? What if Dutch paedophile grooms Belgian netlog site? Racist blog reply from German on Belgian blog?
- International private law, territoriality of criminal law, etc. to be further examined.

High level analysis use cases



Paedophilia

- *Use cases*
 - Grooming by paedophiles;
 - The sexual harassment of children and young people; and
 - The posting of photographs or videos of naked or semi-naked adolescents, *by adults*.
- *Analysis*
 - Criminal procedural law: to be further examined to which extent private parties may get involved in tracing offences (similar to "vigilante" - neighbourhood watches), and to which extent this is the sole prerogative of the police and judicial authorities

Cyberbullying

- *Use cases*
 - Psychological trauma caused by cyberbullying; and
 - Frequent breaches of privacy, reputation and personal dignity.
- *Analysis*
 - Between adolescents
 - On the workplace
 - Question arises to which extent Collective Labour Agreement n° 81 applies, and accordingly, to which extent "cyberbullying" is one of the allowed purposes under CBA n° 81
 - The "Anti-bullying Act" contains specific rules and regulations regarding bullying on the workplace
 - Implementation of such a



Media posted by adolescents

- *Use cases*
 - The posting of photographs or videos of naked or semi-naked adolescents, *by themselves or other adolescents*;
 - The posting of pictures or movies showing self-mutilation.

- *Use cases*
 - Explicit advertisements for prostitution and "escort" services;
- *Analysis*
 - A distinction needs to be made between (i) advertisements by adults posted on websites which are often visited by adolescents; and (ii) adolescents offering "escort" services themselves
 - (i) seems to relate to mere contractual arrangements between the website holder and advertisers
 - (ii) question arises as from which moment such behaviour becomes problematic (e.g. a young girl offering her "services" to a boy (of two years older) who she considers to be her (boy)friend, versus a young girl offering her "services" to an adult)
- Arts. 379 et seq. Penal Code apply to enticing a minor to prostitute him/herself and other related offences

Freedom of speech related use cases

- *Use cases*
 - incitement to violence, racism and xenophobia;
 - dissemination of totalitarian ideologies
- *Analysis*
 - Typically conflict with the freedom of speech
 - With respect to totalitarian ideologies, could possibly amount to "discrimination" (in the sense that, e.g. communist messages are picked up and acted upon by the software)
 - Could cover the prohibition of negationism
 - Could relate to terrorist actions: laws regarding national security could play a role (as from when does "monitoring" become "surveillance"?)

Suicide

- *Use cases*
 - Suicidal behaviour by young people, allegedly as a result of certain intimate details being made public through these networks.
- *Analysis*
 - Major liability issue (bodily injury and death)

- Q&A

