Data Protection & ISP Liability from an International Perspective

WOLF THEISS

Lukas Feiler, Ph.D., SSCP
Associate, Wolf Theiss Attorneys at Law

TOPICS

WOLF THEISS

Data Protection Law
- Regulatory approaches in the EU and the U.S.
- Roles and responsibilities
- Regulatory requirements for processing data
- Outsourcing
- Legal consequences of non-compliance
- Cloud computing

ISP Liability
- Types of ISPs and sources of liability
- Liability exemptions
- Injunctions for defamatory or libelous content
- Injunctions under copyright law

Data Protection as a Fundamental Right in the EU

WOLF THEISS

- European Convention on Human Rights
  - protects privacy (article 8)
- EU Charter of Fundamental Rights
  - specifically provides the right to data protection (article 8)
- Austria: Data Protection Act § 1
- Germany: Fundamental right of informational self-determination

Data Privacy under U.S. Law

- Constitutional Law
  - 1st Amendment: Freedom of association covers confidentiality of membership list (NAACP v. Alabama, 357 U.S. 449 (1958)
  - 4th Amendment: Protection against unreasonable searches & seizures; however only if there is a "reasonable expectation of privacy" (Katz v. United States, 389 U.S. 347 (1967))
    → secrecy paradigm

Data Privacy under U.S. Law #2

- Federal law
  - only sector-specific and in reaction to specific incidents, e.g.:
    - Health Insurance Portability and Accountability Act: health care providers
    - Gramm-Leach-Bliley Act: financial institutions
    - Fair Credit Reporting Act: credit reporting agencies
    - Video Privacy Protection Act: video tape service providers
  - largely: self-regulation
- Common law / privacy torts
  - intrusion upon seclusion → secrecy paradigm
  - public disclosure of private facts → secrecy paradigm

Is Privacy Dead?

- "You have zero privacy anyway, get over it"
- Millions of users have public profiles on Facebook
- Do consumers still value privacy?
  - Depends on the context!
  - "Privacy in Context": consumers may be willing to share their data in one context while refusing to do so in another context
    - some people may share information on their religious beliefs with their friends but not their co-workers
    - while sharing information about their income with their co-workers but not their friends
  - Facebook: private context (family, friends, acquaintances)
  - Google+: circles attempt to replicate "spheres of life"

The Legal Framework of Data Protection in the EU

- Data Protection Directive (Directive 95/46/EC)
- ePrivacy Directive (2002/58/EC) – generally only applies to the telecommunications sector
- On the horizon: a new General Data Protection Regulation that would repeal the Data Protection Directive

What is "Personal Data"

Data Protection Directive

- any information relating to an identified or identifiable natural person
- an identifiable person is one who can be identified, directly or indirectly

Member States' Laws

- Some Member States – in particular Austria – differentiate:
  - personal data: the data subject can be identified
  - indirectly personal data: data subject cannot be identified by the entity collecting the data (using legal means)

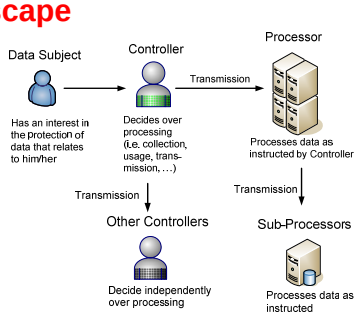
  → "personal data" becomes a relative term; it might be "personal data" for one company but is "indirectly personal data" for another

Actors in the Data Protection Landscape

- "Data subject"
  - Data Protection Directive: a natural person to whom the information relates
  - Austria, Italy & Luxembourg: legal persons are covered too
- Controller
  - Entity which determines the purposes and means of the processing of personal data
- Processor
  - Entity which processes personal data on behalf of a controller

    → i.e. service providers

Actors in the Data Protection Landscape



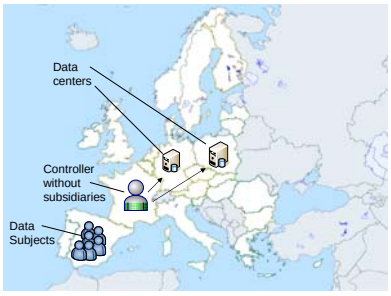
Regulatory Authorities

- National Supervisory Authorities
  - EU data protection law is exclusively enforced by these national authorities
- European Data Protection Supervisor (EDPS)
  - monitors the compliance of processing operations carried out by an EU institution (European Commission, European Parliament, Council, …).
  - Advises EU institutions in legislative affairs
- "Art 29 Working Party"
  - Consists of representatives from the National Supervisory Authorities
  - Advises the European Commission & the Supervisory Authorities

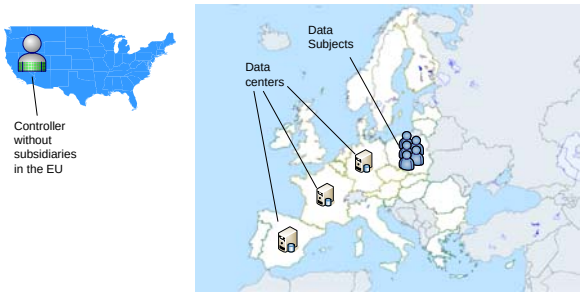
National Data Protection Laws Differ even in the EU – Which one applies?

- Principle: Location of the controller's establishment is decisive (art. 4)
  - E.g. if XZY GmbH offers web services in the entire EU but only has an establishment in Austria, only Austrian law applies
- If the controller has multiple establishments in the EU:
  - In the context of the activities of which establishment is the processing carried out?
  - E.g. the parent company implements a single CRM solution for all its establishments in the EU → each establishment has to comply with local law
- If the controller has no establishment in the EU
  - Has to comply with the laws of all Member States in which processing equipment is used

Which Law Applies?



Which Law Applies?



Requirements for Processing Personal Data

General principles (art. 6)

- Data must be processed
  - Fairly: proportionality of conflicting interests to be maintained
  - Lawfully: processing requires a legal basis
- Purpose limitation: data may only be collected for a specified and legitimate purpose and must not be processed in any way incompatible with that purpose
- Data minimization: data must be relevant for the defined purpose
- Accuracy: data also has to be kept up to date
- Time limit of data storage: only as long as required by the defined purpose

Requirements for Processing Personal Data

WOLF THEISS

Personal data may only be processed if one of the following applies (art. 7):

1) The data subject has given his consent
   Requirements:
   - specific & informed consent
     - Which data elements?
     - For what purpose?
   - does not have to be express; implied consent is sufficient (if no sensitive data is involved)
   - does not have to be in writing
   - consent may also be withdrawn at any time ("right to be forgotten")

Requirements for Processing Personal Data #2

WOLF THEISS

Personal data may only be processed if:

2) Processing is necessary for the performance of a contract
   - E.g. billing & address information has to be processed in order to perform a distance sales contract

3) Processing is necessary for the controller to comply with legal obligations
   - Excludes obligations under a contractual or non-EU-MS law
   - E.g. record-keeping obligations of a corporation

4) Processing is necessary to protect vital interests of the data subject
   - E.g. disclosure of family records to find potential organ donor for data subject who is in a coma
   - Learning about the controller's latest product: not a vital interest!

Requirements for Processing Personal Data #3

WOLF THEISS

Personal data may only be processed if

5) Processing is necessary for performance of a governmental task carried out in the public interest
   - Very rare in the private sector

6) Prevailing legitimate interest of the controller or of third parties
   - E.g. controller has to use the personal data to prove a claim against the data subject in court (cf. Austrian Data Protection Act § 8(3)(5))
   - E.g. implementing a whistleblower hotline as required under the U.S. Sarbanes-Oxley Act (SOX)
   - E.g., in some Member States: only indirectly personal data such as IP addresses in a webserver's log file

Requirements for Processing Sensitive Personal Data

WOLF THEISS

Sensitive data ("special categories of data"): personal data revealing (art. 8)

- ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade-union membership; or
- data concerning health or sex life.

In some Member States (e.g. Austria) personal data relating to criminal offences is treated similarly as sensitive data.

Requirements for Processing Sensitive Personal Data #2

WOLF THEISS

Sensitive data may only be processed in the following cases:

1) Data subject has given his or her explicit consent
   - E.g. by ticking a check-box on a website
2) Processing in the context of employment if authorized by Member State law
3) Processing is necessary to protect vital interests of the data subject if the data subject is incapable of giving consent
4) Ideological associations' privilege: they may process sensitive data of their members in the course of their legitimate activities
   - E.g. a trade union may process the membership status of their members

Requirements for Processing Sensitive Personal Data #3

WOLF THEISS

Sensitive data may only be processed if:

5) The personal data has been made public by the data subject
   - E.g. information on public Facebook profile pages
6) Processing is necessary for establishment/defense of legal claims

Excursion: Processing Employee Data

- Employment law differs in each Member State
- Principles in Austria
  - Surveillance that violates human dignity is prohibited, irrespective of anybody's consent
    - e.g. video surveillance in the bathroom
  - Surveillance that interferes with human dignity
    - Requires the consent of the workers' council, if there is one (§ 96 ArbVG)
    - If there is no workers' council, individual consent has to be obtained from every employee (§ 10 AVRAG)
    - E.g. monitoring employees' Facebook activities; monitoring employees' email or telephone communication

Excursion: Processing Employee Data – Whistleblowing Hotlines

- U.S. Sarbanes-Oxley Act requires publicly listed companies to implement a whistleblowing system
- Permissible under EU data protection law?
  - necessary for the controller to comply with legal obligations (art. 7(c))?
    - No, since foreign legal obligations are irrelevant
  - Prevailing legitimate interest of the controller (art. 7(f))?
    - good corporate governance vs. employee privacy
    - Possible, but proportionality, subsidiarity, and the seriousness of the alleged offences that can be notified have to be considered
    - Cf. Opinion 1/2006 of the Article 29 Working Party

Obligation to Notify the National Supervisory Authority

- Controller has to notify Supervisory Authority prior to starting any data processing operations (art. 18)
- Notification has to include (art. 19)
  - controller's name and address
  - the purpose of the processing
  - a description of
    - the categories of data subjects; and
    - the categories of data relating to them
  - the (category of) recipients to whom the data might be disclosed
  - general description of security measures

Notified Processing Operations & National Data Processing Registers

- Each Member State maintains a Data Processing Register (art. 21)
  - register is publicly accessible
  - contains all notified information except security information
  - In practice: some Member States (e.g. Austria) do not make the Register available online, reducing the transparency it creates in practice
  - In some Member States (e.g. Austria) the register number (DVR-Nr.) has to be included in all communications to data subjects

Exemptions from the Notification Obligation

- Member States may exempt a processing operation from the notification obligations if
  - the processing operation is unlikely to affect the rights of data subject
    - e.g. in Austria: Standard and Template Regulation (Standard- und Musterverordnung 2004) – the following do not have to be notified (e.g.):
      - Accounting and Logistics
      - Personnel Management

      the following can be notified easier (only name of controller and processing operation needed; e.g.)
      - Access Control System (for physical access to a building)

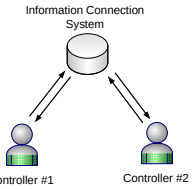
Exemptions from the Notification Obligation #2

- Member States may also exempt a processing operation from the notification obligations if
  - the Controller has appointed a Data Protection Officer (DPO)
    - DPO is responsible for
      - ensuring compliance of the Controller
      - keeping an internal data protection register of the controller's processing activities
    - DPO has to be completely independent

    → e.g., Germany has implemented this exemption; Austria did not

Processing Requiring to Prior Authorization

- Some processing operations are so risky as to require prior authorization from the National Supervisory Authority (art. 20)
  - e.g., in Austria, prior permission is needed if
    - multiple controllers feed data into and access data from the same data processing operation ("Informationsverbundsystem")



Information to be Given to Data Subjects

- A Controller has to inform at least about (art. 10 & 11)
  - its name
  - the purposes of the data processing
  - the (categories of) recipients of the data
  - If required under national law
    - in a questionnaire: whether replies to the questions are obligatory or voluntary & possible consequences of a failure to reply
    - the existence of the right of access to and the right to rectify data concerning the subject

Data Subjects' Rights – The Right of Access

- A data subject has to right to
  - receive confirmation as to whether his or her data is being processed
  - obtain information about
    - the purposes of the processing,
    - the categories of data concerned, and
    - the (categories of) recipients
  - receive
    - a copy of his or her personal data "in an intelligible form"
      → data portability?
    - information about the data's source

Data Subjects' Rights – The Rights of Rectification, Erasure & Blocking

- A data subject has to right that her personal data is
  - rectified if it was not accurate or up-to-date
  - erased or blocked if it is otherwise not in compliance with the Directive
- A data subject may also demand the notification of the rectification/erasure/blocking to third parties to whom the data has been disclosed

→ Is there an effective right to be forgotten?

Data Subjects' Rights – The Right to Object

- If grounds for legitimacy of processing were something other than the data subject's consent
  - Member States have to provide the right to object in particular if
    - Grounds for legitimacy were the prevailing legitimate interest of the controller or of third parties
    - data is used for direct marketing
  - personal data of the objecting individual have to be excluded from further processing operations if objection is justified

Security of Personal Data

- What is "security"?
  - **C**onfidentiality
  - **I**ntegrity
  - **A**vailability
- How do we measure whether something is secure?
  - Security is never 0 or 100 / yes or no
  - Security is measured in terms of risk
  - How high is a "security risk"?
    → Risk = impact x probability
    → Annualized Loss Expectancy (ALE) =
    Annualized Rate of Occurrence (ARO) x
    Single Loss Expectancy (SLE)

Security of Personal Data

- Security of processing (art. 17)
  - Controller must implement "appropriate" technical and organizational measures to protect personal data against
    - accidental or unlawful destruction or accidental loss → Availability
    - alteration → Integrity
    - unauthorized disclosure or access → Confidentiality
  - "Appropriate": to be determined by
    - the risk presented by the nature of the data
    - the cost of the security measures → cost/benefit analysis

Security Breach Notification

- *The duty to notify individuals if the security of their personal data has been breached.*
- A policy invention made in California
  - California Senate Bill 1386 (2002)
- Purpose:
  - Affected individuals should be able to take reactive measures
  - Market transparency as regards information security
- Legal sources of a notification duty
  - General data protection law
  - Telecommunications law
  - Contract law

Security Breach Notification under Data Protection Law

- Data Protection Directive: does not require notifications
- National laws:
  - Austria: If the controller learns that personal data is "systematically and seriously misused" and the data subject may suffer damages (Austrian Data Protection Act § 24(2a))
  - Germany: If a third party unlawfully obtains knowledge of certain types of sensitive data and a "severe interference" with the rights of data subjects may occur (German Federal Data Protection Act § 42a)

Security Breach Notification under Telecommunications Law

- Art 4 of the e-Privacy Directive (2002/58/EC) requires:
  - Notification to the national regulatory authority
    - of any breach of security leading to the accidental or unlawful destruction, loss, alteration, disclosure of, or access to, personal data
  - Notification to the data subjects
    - if breach is likely to adversely affect the personal data or privacy
- Proposed General Data Protection Regulation contains identical notification duty

Security Breach Notification under Contract Law

- Austrian law: contractual duty to notify
  - Implied duty to prevent harm to the other contracting party
  - Breaches have to be notified if there is a risk of harm
  - Determining the limits of this duty
    - Implied duties are inherently vague
    - Duty should be regulated/limited by specific contractual provisions
  - Consequences of a failure to notify: contractual liability for economic losses

The Potential Effects of Security Breach Notification

- Reduction of information asymmetry
  - Customers typically have no information about the security of an online service – however, the service provider does
  - Breach notifications introduce transparency and thus increase competition regarding IT security
  - Opportunity for corporations with good security
- Internalization of the data breach risk
  - Until now: security breach was largely an externality for the company
  - Now: Company has to bear larger share of the negative effects of a breach

Crisis Communication after a Security Breach

- How not to act
  - Claiming that no personal data was affected when indeed it was, thereby challenging hackers to publish data as proof
- Efficient crisis communication requires that you already know how to fulfill your notification obligations
  - What type of personal data is maintained by the corporation?
  - Is the data encrypted? If so, how strong is the encryption?
  - How sensitive is the data?

Most of these questions can be answered *in advance.*

Outsourcing – Transmission of Data to a Processor

- Controller may out-source data processing operations to a Processor
  - Transmission has to be justified like any other processing operation
    - typically prevailing legitimate interest of the Controller
    - → in general, data subjects' consent not needed
  - Outsourcing has to be governed by a contract

Outsourcing – Transmission of Data to a Processor #2

- Mandatory content of an outsourcing contract (art. 17)
  - Obligation of the Processor to only process data as instructed by the Controller
  - Obligation of the Processor to implement appropriate security measures
- For purposes of keeping proof, outsourcing contract has to be in writing

Outsourcing to Non-EU Processors

- Outsourcing to processors not established in the EU
  - Principle: only permissible if the third country ensures "an adequate level of protection"
    - Europ. Commission has designated a number of third countries as providing "adequate" protection
    - e.g., the U.S.:
      - Safe Harbor program
      - "adequate" protection is provided if
        - » the Processor has self-certified compliance with the safe harbor rules → safeharbor.export.gov/list.aspx
        - » enforcement: FTC Act § 5

Outsourcing to Non-EU Processors

- Outsourcing to processors not established in the EU
  - Exceptions: transmission permissible despite lack of "adequate level of protection" in non-EU country if
    - data subject has consented to transfer
    - transfer is necessary to protect the vital interests of the data subject
    - outsourcing contract contains standard contractual clauses adopted by the Commission

Legal Consequences of Non-Compliance

- Administrative penalties
  - All Member States provide penalties for non-compliance
    - In Austria: up to EUR 25,000 for each infringement
- Civil Liability
  - Data subjects may recover damages suffered as a result of an unlawful processing operation
  - Also immaterial damages?

Cloud Computing – A New Form of Outsourcing

- Types Cloud Computing
  - Infrastructure as a Service (IaaS)
    - Vendor provides (virtualized) hardware
  - Platform as a Service (PaaS)
    - Vendor provides (virtualized) hardware + runtime
  - Software as a Service (SaaS)
    - Vendor provides (virtualized) hardware + runtime + application software
- Private vs. public cloud
  - Private cloud: e.g. operated by your own IT department
  - Public cloud: outsourcing!

Cloud Computing – Risks and Opportunities

- Opportunities
  - Reduced total costs of ownership (TOC)
  - Scalability & flexibility
- Risks
  - Availability
    - How good is your Internet connection?
    - what if the cloud service provider goes bankrupt?
  - Integrity
    - How good are the provider's backup & restore mechanisms?
  - Confidentiality
    - How well is one user shielded from another?
    - How does authentication work? Who else has access?

Cloud Computing – Legal Challenges

- Providers of a public cloud are Data Processors
- Cloud Computing agreement has to meet minimum content requirements
  - Obligation of the Processor to only process data as instructed by the Controller
  - Obligation of the Processor to implement appropriate security measures
  - → What if standard terms & conditions (T&C) offered by the provider do not meet the requirements?
  - → What if the T&C allow the provider to do processing for its own purposes?

Cloud Computing – Legal Challenges #2

- How can the Controller verify the adequacy of the security measures?
  - Cloud computing provider should be obligated to comply with recognized standard (e.g. ISO/IEC 27001)
  - Compliance with security standard should be verified and certified by independent third party
  - Pitfalls
    - When does the certification expire?
    - What is the scope of the certification?
    - Who is the certifying authority?

Cloud Computing – Legal Challenges #3

- Transmission to a cloud computing provider in a non-EU country
  - General requirements apply:
    - Third country has to provide adequate protection (e.g. U.S. Safe Harbor self-certification); or
    - Commission-approved standard contractual clauses have to be used
  - What if it becomes impossible to tell where in the world your data is?
    - Standard contractual clauses are needed

Cloud Computing – Legal Challenges #4

- Data portability and lock-in
  - How do you get your data to a different provider?
    - SaaS Cloud computing contract should provide a right to get your data in a structured data format
  - Costs of transferring your data = “switching costs”
    - It will only make sense to change to a different provider if the switching costs are not higher than financial advantages offered by the new provider

Cloud Computing – Access by Foreign Governments

- Government authorities can ask for and enforce access to the cloud if
  - The cloud service provider is established in that country
    → penalties can be assessed and directly enforced
  - The cloud service provider operates data centers in that country
    → the physical servers can be seized

Cloud Computing – Access by Foreign Governments #2

- USA PATRIOT Act § 505: National Security Letters
  - For all transaction data (no contents of communications)
  - No judicial oversight
  - Secrecy obligation ("gag orders")
- EU Data Protection Law
  - All interferences with the fundamental right to data protection have to be proportional
  - There has to be an effective judicial protection

Cloud Computing – Access by Foreign Governments #3

For example:

- A U.S.-based cloud service provider functions as a processor for a controller in the EU
  - Data protection law of the respective Member State applies
- Since the provider is established in the U.S., it is subject to USA PATRIOT Act § 505

→ U.S. law mandates the violation of EU law
→ EU law mandates the violation of U.S. law

Liability of Internet Service Providers

- What is an ISP?
  - Internet access provider
  - Hosting provider (hosting third party content)
  - Caching provider (caching third party content)
  - Search engine

→ Most companies function as a hosting provider
- Hosting any user-generated content on their website
- Operating a company Facebook page

→ Most companies also function as an Internet access provider
- Providing Internet access to employees & guests

Liability of Internet Service Providers

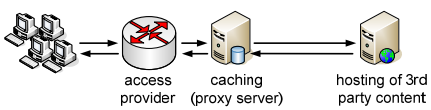
- Why do ISPs face liability risks?
  - ISPs are intermediaries
  - in contrast to the primary infringer they are
    - easy to identify
    - often established in the victim's jurisdiction

- Legal basis of liability
  - Primary liability: making infringing content publicly available
    - E.g. copyright infringement
    - E.g. defamation & slander
  - Secondary liability: ISPs contribute to the infringement by their users by making their services available to them

Liability of Internet Service Providers

- The E-Commerce Directive provides exemptions from liability for
  - Internet access services (mere conduit)
  - Caching services
  - Hosting services

The exemptions apply to all areas of the law, including intellectual property law



Liability Exemption for Internet Access Providers

- An Internet access provider is not liable for the information transmitted if it (E-Commerce Directive art. 12)
  - does not initiate the transmission;
  - does not select the receiver of the transmission; and
  - does not select or modify the information contained in the transmission.
- Result: No liability even if Internet access provider has actual knowledge of infringing content

Liability Exemption for Caching Providers

- A caching provider is not liable for the information temporarily stored if it (E-Commerce Directive art. 13)
  - does not modify the information;
  - complies with conditions on access to the information
  - complies with common rules on updating of the information
  - does not interfere with the lawful use of technology commonly used to obtain data on the use of the information;
  - expeditiously removes information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed
- Result: No liability even if caching provider has actual knowledge of infringing content

Liability Exemption for Hosting Providers

- A hosting provider is not liable for the information stored if it (E-Commerce Directive art. 14)
  - is not aware of facts or circumstances from which the illegal information is apparent; or
  - upon obtaining such awareness acts expeditiously to remove or to disable access to the information
- Result: Notice and take-down regime

Hosting Providers: Implementing a Notice-and-Take-Down Regime

- Provide a clear & easy-to-use notice mechanism
  - e.g. a "report this posting" button
- Diligently monitor alternative notice mechanisms
  - e.g. emails sent to abuse@<COMPANY>.com
- Ensure that specifically trained personnel monitor the notice mechanisms
- Take infringing content offline right away
  - How to act in the grey area?
  - Potential liability vis-à-vis the victim
  - Potential liability vis-à-vis the user whose content is taken down
  - Public relation challenges:
    - "promoting infringement" vs. "censorship"

Liability Exemptions for ISPs under U.S. law

- Communications Decency Act
  - Covers all "interactive computer service providers"
  - no liability, even if knowledge of the information in question (Zeran v. Am. Online, Inc., 129 F.3d 327 (4th Cir. 1997))
  - does not apply with regard to "any law pertaining to intellectual property"
- Coypright Act § 512 – similar to the E-Commerce Directive but
  - Hosting provider: "willful blindness" may constitute knowledge (Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19 (2d Cir. 2012))
  - No safe harbor for vicarious liability (right and ability to supervise & direct financial interest)

Injunctions Against ISPs

- E-Commerce Directive states that the liability exemptions
  - *shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement*
- Injunctive relief is therefore available against ISPs

Injunctions for Defamatory or Libelous Content

- Guestbook Judgment of the Austrian Supreme Court (6 Ob 178/04a)
  - Tourist organization operated a guest book on its website
  - User "Chris" created a posting that damaged a hotel's reputation and creditworthiness
  - Hotel sent a take-down notice to the tourist organization which deleted the posting right away
  - Other users then created further postings
    - complaining that Chris' posting was taken offline and
    - repeating the previously deleted infringing statements

Injunctions for Defamatory or Libelous Content #2

- Guestbook Judgment of the Austrian Supreme Court (6 Ob 178/04a)
  - The Court held:
    - Further infringements were to be expected after the first posting since it invited comments
    - After having been notified of first infringement, website operator was obligated to
      - continuously monitor the guest book for any further infringements of the same kind and
      - delete them without undue delay
  - Injunction was issued that required website operator to prevent any similar infringements

Injunctions under Copyright Law

- Copyright Directive (2001/29/EC) art. 8(3) provides
  - *Member States shall ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right.*
  - Case C-324/09, L'Oréal SA v. eBay: injunctions are not limited to measures which contribute to bringing infringements to an end but may also cover measures which contribute to preventing further infringements of that kind.

Injunctions under Copyright Law – Important Issues

- Are Internet access providers “intermediaries”?
  - Case C-557/07, LSG v. Tele2: Yes!
- Are hosting providers “intermediaries”?
  - Case C-360/10, SABAM v. Netlog: Yes!
- What levels of monitoring are required to prevent future infringements?
  - Case C-360/10, SABAM v. Netlog: full-scale content filtering system on social networking website would violate fundamental rights
  - Case C-70/10, Scarlet Extended v. SABAM: active monitoring of all customer traffic would violate the fundamental rights

Website Blocking Injunctions under EU Copyright Law – ECJ Case Law

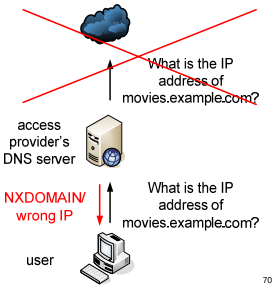
- Injunctions against Internet access providers, ordering them to prevent their subscribers from accessing certain websites
- Case C-70/10, Scarlet Extended v. SABAM: active monitoring of all traffic data would violate the fundamental rights
  - of the ISP concerned to conduct its business;
  - of users to receive or impart information; and
  - of users to protection of personal data
- Is a website blocking injunction a similarly severe interference with fundamental rights?

How to Implement Website Blocking Injunctions

- Three basic possibilities
  - DNS blocking
  - IP blocking
  - Proxy

Implementing Website Blocking Injunctions – DNS Blocking

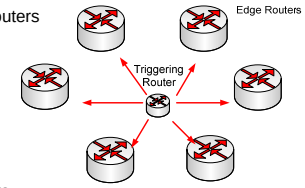
- The access provider's DNS server has to be reconfigured
- Possible circumvention
  - For users:
    - alternative DNS server
    - use IP address
  - For website operators
    - Choose different domain



Implementing Website Blocking Injunctions – IP Blocking

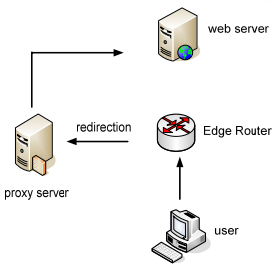
IP blocking via remote-triggered black hole filtering

1. Configure a static route to Null0 Interface on all Edge Routers (e.g. for 192.0.2.0/24)
2. At the Triggering Router: configure e.g. 192.0.2.1 as next hop for the IP address to be blocked
3. Distribution of the routing information to all Edge Routers via iBGP



Implementing Website Blocking Injunctions – Proxy

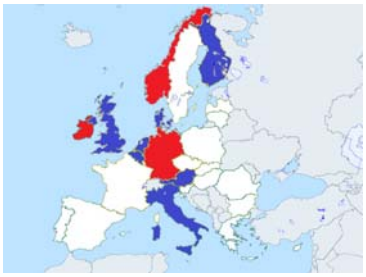
- All traffic is routed over a proxy server
  - It can perform filtering base on URLs or content
  - Problem: encryption
- Costs for access provider
  - Very high
- Possible circumvention
  - For users similar to IP blocking



Website Blocking Injunctions under EU Copyright Law – Nat'l Case Law

Injunctions issued
- Austria
- Belgium
- Denmark
- Finland
- Italy
- Netherlands
- U.K.

Injunctions denied
- Germany
- Ireland
- Norway (Non-EU-MS)



Website Blocking Injunctions under U.S. Law

U.S. Copyright Act § 512(j)(1)(B)(ii): A court may grant injunctive relief in the following form:
- *An order restraining the service provider from providing access, by taking reasonable steps specified in the order to block access, to a specific, identified, online location outside the United States.*
- So far, only a single case: Arista Records, Inc. v. AT&T Broadband Corp., No. 1:02CV06554, 2002 WL 34593743 (S.D.N.Y. Aug. 16, 2002)
  - Plaintiffs sought an injunction against Internet backbone operators to block the Chinese website Listen4Ever
  - Complaint was voluntarily withdrawn

Thank you!

Contact Details

WOLF THEISS

Lukas Feiler, Ph.D., SSCP

Wolf Theiss Attorneys at Law
Schubertring 6, 1010 Vienna

Tel: (+ 43 1) 515 10 5090
Fax: (+ 43 1) 515 10 665090

e-mail: lukas.feiler@wolftheiss.com

www.wolftheiss.com