SLW INSTITUTE

GLOBAL IP CONFERENCE

with Advanced PCT Training | 2018

Track I: Global IP Strategies

Top Five IP Interactions with GDPR

Presenters

Liz Fortier

Vice President &
General Counsel, *Lucid*

Mark Stignani

Analytics Chair &
Compliance Officer, *Schwegman*

SLW INSTITUTE
GLOBAL IP CONFERENCE
with Advanced PCT Training | 2018

What are we Teaching???

- GDPR basics
- Top 5 Interactions with IP
- 5 Unknowns of the GDPR
- In-house v. Law Firm Reflections
- What's Next

What is the GDPR's Purpose?

- **EU People Have Power Over Their Personal Data**
  - EU citizens have individual rights exceeding any claims made by any company
  - Requires company follows guidelines on tracking the collecting, processing or storing of EU citizens personal data
    - Requires full disclosure from the company regarding how they will use your personal data once it is collected
    - Requires all the privacy notices that oversee consumer data are easy to read and understand
    - Requires an easy and straightforward way for them to opt out and erase their personal data without undue delay
  - GDPR levies large fines for non-compliance

What are the Penalties?

- The maximum amount of financial sanctions is increased up to 4% of total worldwide annual sales
- 20 million Euros

Whichever Is The Greater

Who is Affected by GDPR?

- Extraterritorial Effect
  - The GDPR extends the application of EU legislation to companies outside the EU, in that it will apply to entities established outside the EU that offer goods or services to individuals in the EU and/or monitor the behavior of data subjects within the EU
- Anyone with EU citizens as:
  - Customers
  - Employees
  - Clients
- Vendors who sell services to the previous bullet(Law Firms)

Controller/Processor

- **Controller definition**
  - means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- **Obligations**
  - According to Article 5 from the EU GDPR, the controller shall be responsible for, and be able to demonstrate compliance with, the principles relating to processing of personal data. These are: lawfulness, fairness and transparency, data minimization, accuracy, storage limitation and integrity, and confidentiality of personal data.
  - According to Article 24 from the EU GDPR, "*Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.*"

- **Processor definition**
  - *means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*
- **Obligations**
  - According to Article 28 from the EU GDPR, "*Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.*"
  - This means that if any EU or non-EU company wants to stay in business, as controller or processor, it will have to implement the necessary controls to ensure that they comply with the EU GDPR, because the fines can be applied to both controllers and processors. According to Article 83, fines shall be imposed regarding "*the degree of responsibility of the controller or processor taking into account technical and organizational measures implemented by them.*"

GDPR Personal and Sensitive Data

- Personal data is any information related to an identified or identifiable natural person That can include both direct identification (such as, your legal name) and indirect identification (such as, specific information that makes it clear it is you the data references) The GDPR also makes clear that the concept of personal data includes online identifiers (such as, cookies, IP addresses, mobile device IDs) and location data
- Sensitive data includes specific definitions
  - genetic data and biometric data Sensitive data also includes racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership:
  - data concerning health; or data concerning a person's sex life or sexual orientation) are treated as sensitive personal data under the GDPR
- Sensitive personal data is afforded enhanced protections and generally requires an individual's explicit consent where these data are to be processed

IP Interactions with GDPR

That we know of today…

SLW INSTITUTE
GLOBAL IP CONFERENCE
with Advanced PCT Training | 2018

IP Interaction (IPI) #1: Inventor Address

- Under the GDPR, a corporate applicant may not disclose personal data of EU resident-inventors without their documented affirmative consent which can be easily withdrawn
- If an inventor objects to the disclosure of information pursuant to the GDPR, an EU corporate assignee is placed in the untenable position of having its patent applications in the United States refused or denied because they fail to meet regulatory requirements or facing monetary penalties in the EU and being forced to withdraw the disclosed personal information in addition to civil remedies
- A person can even exercise the “right to be forgotten” under the GDPR and demand that their personal data be erased Generally, the GDPR applies to EU organizations as well as non-EU organizations that provide services or goods in the EU
- Upon objection by an employee-inventor, an EU corporation (or even a U S corporation with EU resident employee-inventors) would be precluded under the GDPR from disclosing any information relating to the residential address of the objecting inventor

IPI #2: Data Portability

- The right to portability is a new right that did not exist before the GDPR
  - Purpose to help data subjects switch from one supplier to another
  - Data subjects have the right to receive their personal data in a structured, commonly used and machine readable format, which they can then forward to someone else(Facebook)
- "Someone else" may be a competitor, the right to portability raises issues for those who may take the view that providing personal data in a "reusable way for potential competitors" would be an infringement of their IP rights or, at the least, a disclosure of their know-how (Invention disclosures?)
  - But GDPR provides that the exercise of this right "should not adversely affect the rights and freedoms of others," which include IP rights
- Scope of data portability is limited to the raw personal data provided by the data subjects themselves, and should not include data which is inferred or derived from the raw data
  - Much company IP emerges after raw data transforms to more valuable metadata

IPI #3: Right of Access

- The “right of access” already exists under EU law in the Directive Pursuant to the right of access, individuals (in the data protection jargon, they are called “data subjects”) can obtain a copy of all the personal data that has been collected about them
- GDPR provides, as a derogation to the exercise of the right of access, that it “*should not adversely affect the rights or freedoms of others,*” including trade secrets and intellectual property rights, in particular with respect to software
- These considerations will limit the information available to a data subject, but will not justify a refusal to provide any information

IPI #4: Data Protection v DRM/Profiling

- For companies that use profiling, it is important to keep in mind the following GDPR requirements:
  - All processing activities must have a legal basis, such as the consent of the data subjects or the fact that the profiling is necessary in order to provide the service For example, the insertion of a unique identifier in a content protected by copyright via a Digital Rights Management scheme should not be linked to an individual except to the extent that this link is necessary for the performance of the service or if the individual has been informed and has consented to it
  - You cannot use personal data for purposes that are not compatible with the purpose for which the data was originally collected For example, if you sell goods to customers who pay with credit cards, you may collect their name and address but you cannot use them later for marketing purposes
  - Personal data should not be stored longer than is necessary to fulfill the purpose for which such data is processed For example, if you collect personal data about your customers, you must delete that data as soon as it is no longer necessary for billing purposes or any other purposes (after-sale services) consented to by the customers You cannot keep the data “just in case” one of them might misuse your IP

IPI #5: Privacy v Enforcement of IP Rights

- EU Litigation Discovery can open a GDPR issue
  - When IP owners conduct investigations to identify potential infringers, they are collecting and processing personal data
    - Who is doing extraction – processor v. controller
    - Linkedin profiles
    - Other public data that can lead to a inference

- IP Litigation will create a potential conflict between the protection of IP rights and the protection of personal data, which requires that data be only processed when there are appropriate safeguards and transparency

Unknowns in GDPR at this Point

Potential Weaknesses or Loopholes

Potential Unknowns in GDPR

- With any new piece of legislation
  - Law of unintended consequence
  - Oversimplification of the problem
  - Global nature of the problem
- 5 Potential Unknowns

Potential Unknown (PU) #1: Data Escape

- The GDPR is meant to protect people in the EU when their personal data is controlled by organizations outside the EU
- Wording of the law(Recital 23) may allow data to "escape" the GDPR if it passed on to others without legal protection
- Likely will not help social media monitoring under Article 3 2(b)

PU #2: Data that Loses GDPR Protection

- Even if data is collected and processed legally under the GDPR, it can be transferred to others and then escape the protection of the law
- Non-EU data "controller" (an entity that processes data), it is only subject to the GDPR when *the processing activities are related to the offering of goods or services* to the individual in the EU (or monitoring the behavior of the person), the same personal data could be processed for another purpose without being subject to the GDPR

PU #3: Non-Obvious Controller

- If organizations obtain data indirectly, in most cases it should still be subject to the GDPR
- Data collection is many faceted & non-obvious
  - Discovering which controller is collecting maybe difficult
  - Ad Tech & Browser Trackers (1726 individual trackers)
  - Article 15 covers access request inquiries (which tracker when?)
  - No obligation on the controller to inform the data subject that any profiling is taking place — unless it produces “legal effects…or similarly significantly affects him or her”

PU #4: Inferred/Derivative Data

- Personal data is any data related to a living person The GDPR gives obligations to processors of the data and it gives rights to individuals
- Users may lose a number of rights when a company extracts and derives metadata, but complies with GDPR

PU #5: Legitimate Interests

- It may seem reasonable that organizations should be able to process personal data if they have a good reason to do so, *after considering the interests of the individuals involved…*
- legitimate interests of the organization processing personal data has not changed from the 1995 data protection Directive, and the wording of the provision in the GDPR is almost identical
- It requires that the controller balances its own (or a third party's) legitimate interests against the interests or fundamental rights and freedoms of the data subject

So what do we do?

Must Do's for Compliance

- Audit your processes/data
- Establish a consent process for your Data Subjects
- Use personal data only for what you have consent for
- Record, Record, Record
- Be able to recover and prove your process/data

Hire a DPO

- Data Protection Officer (**DPO**)
  - Charged with making procedural compliance policy
  - Given power to enforce policy
- Reserve budget for compliance or fines

In-house v. Law Firm Reflections

Liz's Reflections & Mark's Reflections

SLW INSTITUTE
GLOBAL IP CONFERENCE
with Advanced PCT Training | 2018

What's Next?

- See who gets charged / fined first
  - See what they do
  - 20M Euro fine pays for a lot of legal services
- Hope that more definition around IP gets written

Questions

Liz Fortier
efortier@luc id

Mark Stignani
mstignani@slwip com

SLW INSTITUTE
GLOBAL IP CONFERENCE
with Advanced PCT Training | 2018