AGON COMPETITION LAW & POLICY PARTNERS
SWITZERLAND

Collection

DATA PROTECTION:

CONFIDENTIALITY DUTIES IN A GLOBAL MARKET PLACE

6th AGON WORKING PAPER
13.3.2015

AGON PARTNERS
Competition Law & Policy – Switzerland
Wiesenstrasse 17
CH-8008 Zürich
www.agon-partners.ch

Legal | Academics | Events | Public Affairs

I. SPEAKERS

Jay L. Himes, Labaton Sucharow LLP (Session's Chair)

Andreas D. Länzlinger, Bär & Karrer (Session's Co-Chair)

Claudia Fritsche, BRP Bizzozero & Partners

Adam Golodner, Kaye Scholer

Claudia Götz Staehelin, Novartis International AG

Jamie Stern, Senior Litigation Counsel, UBS

II. INTRODUCTION

1. After the last networking break, the final group of presenters entered the stage and after a short introduction of the panel members by Mr Himes and Mr Länzlinger, they started their speeches on the topic of data protection and confidentiality duties in a global market place.

III. TOPICS

A. Objectives and raison d'être

2. First, four objectives were defined by Mr Länzlinger. These were subsequently covered by the presentations:

a. Appreciation of the difficulties arising from the interface of jurisdictions with conflicting sets of ground rules

b. Introduction to Swiss law provisions affecting cross-border flow of information

c. Understanding the US stance on cooperation and cross-border flow of information

d. Understanding the limitations and dealing with the challenges. Don't stonewall; find practical solutions

3. He thereafter described the raison d'être of panels in the following manner; as a reaction to the fundamental mismatch between globalisation of business and the globalisation of law and jurisdictions.

B. Problems of cross-border litigation and scenarios

4. To start her presentation, Mrs Götz Staehelin pointed out the fact that some very large multinational companies are based in Switzerland. As they have branches, subsidiaries, employees etc. in different countries, they are affected by different jurisdictional regulations on a

daily basis. This can become extremely difficult as the view on legal issues greatly differs from one country to another. Inter alia, this issue is shown when a European point of view about data privacy is compared to a US one. Such differences bear down intensely when it comes to cross-border litigation.

5. A frequent issue that Swiss companies face is the demand for discovery of Swiss documents for use in a foreign proceeding. For example, when a Swiss company or its foreign affiliate company is served with a US subpoena to hand over documents, cross-border issues come into play as the rules governing such a situation can be completely different. Sometimes, even if you want to comply you may not be able to do so, because you would break the law of your host state.

6. To deal with these problems, we have to understand some singularities and differences which are found in US jurisdictions and compare them to those in Switzerland and other civil law countries.

7. For example, unlike Swizerland, in general the US do not only assume broad jurisdiction over foreign entities and have a different approach to data privacy, but they also know a so-called “cards-on-the-table” approach. This means that there are in particular extensive discovery and information obligations, including broad document requests.These fundamental differences may affect cross-border litigations and fact finding.

C. US perspective

8. The second presentation about the US perspective was presented by Mr Himes.

9. While a full disclosure and full investigatory authority works well within the US or with US based companies, this predisposition will be frustrated in cross-border dealings since there is no possibility of serving a subpoena abroad. Subpoenas served on US soil to business entities with parental structures or affiliates abroad, are subject to special DOJ regulations and procedures. Subpoenas issued with the intent of getting information from abroad are typically called BNS or Bank of Nova Scotia Subpoenas. Nevertheless, there is still a possibility to get to information in a formal way by using one of the many Mutual Law Assistance Treaties (MLAT). However, they are cumbersome and time consuming, and it is far from certain that the investigators will get the information they are looking for.

10. To circumvent this problem, there is a great reliance on informal procedures. There is the possibility of communication between cross-border enforcers or the use of memorandums of understanding (MOUs) with the benefit of higher flexibility and speed, at the cost of quality and quantity of information.

11. The possibility of self-reporting is used as a mechanism to jumpstart the cooperation of a company when beginning an investigation. However, this will not make the investigation any easier. Full cooperation is required, the willingness to end compromising business behaviour and even the willing acceptance of punishment is expected. The investigators will demand a long-term commitment to implement effective compliance programs and lawful business behav-

iour before offering the benefits for turning oneself in. These benefits may include the reduction of fines, deferred prosecution agreements, non-prosecution agreements or in extreme cases can also lead to an investigator foregoing prosecution altogether.

D. Swiss perspective

12. To show the Swiss perspective on cross-border litigation, Mrs Fritsche started by pointing out the Swiss legal barriers to international investigations.

13. Swiss law restricts the sharing of information cross-border. The Swiss blocking statutes pose a challenge to the involved parties, as they face both the danger of civil action and criminal prosecution when sharing cross-border information. Not only are legal entities subject to this danger, but individuals involved in the data transfer process are too. This can include bodies of a company, its litigation counsel and even outside attorneys, in short, everyone involved in the transfer on Swiss territory.

14. Not only does a legal risk have to be managed, but the company's reputation does too. The damage caused by media articles portraying a company as being one which does not protect the data of their clients can be ruinous.

15. There are some main barriers which hinder cross-border information exchange:

a. First of all, it is a criminal offense to carry out activities on Swiss territory for the benefit of a foreign state without permission. These activities include all actions that are reserved by Swiss law for the Swiss authorities e.g. the gathering of evidence. The so-called 271-issue aims to protect Swiss sovereignty. To circumvent this problem, it is necessary to apply for permission or the information exchange has to be kept on an informal level. This is permissible as long as there are no legal consequences and it was not done under duress by a foreign country.

b. Secondly, the provisions against economic espionage have to be considered. It is a criminal offense to probe into business secrets with the intent of disclosing them to a foreign state. This aims to protect the Swiss economy and therefore only the Swiss government can give permission to disclose such secrets and not the owner of the secret!

c. Professional confidentiality and the data protection act have to be respected.

16. To overcome these barriers, a legal solution to each and every one has to be found. To do so, the key is to know the data and to organize it. Depending on the category (e.g. personal data, employee data, business secrets and so on), different solutions will be needed.

17. One safe way to circumvent the 271-issue would be to seek permission from the Swiss authorities directly. As long as you keep to the scope and the conditions of the authorisation you will not be faced criminal proceedings. However, the application of such permissions require a lot of time and are rarely granted.

18. Sometimes it can help to check if it is at all possible to obtain a waiver. In doing so, it is absolutely crucial to clearly define which right should be waived and who the, owner is. Other possibilities include the redaction of documents, the storage of data offshore, outside the Swiss jurisdiction and also to conduct interviews outside of Switzerland.

19. After a solution is found, there are two main channels of data exchange; a partially restricted one inside the multinational company itself and a less rapid and more cumbersome one via the official government channels.

E. Scenarios

20. To allow an in-depth understanding of cross-border litigation issues from a Swiss perspective, a case with four scenarios was presented by Mrs Götz Staehelin and then reviewed by Mrs Fritsche:

21. A US law enforcement agency is investigating a US company for worldwide bribery by its subsidiaries and affiliates. The company is part of an international group with its headquarters in Switzerland, where the records are kept and the top management is located.

22. **S1)** After the proceedings started, the law enforcement agency subpoenaed Swiss residents to testify and give evidence.

23. Two 271-issues arise from this procedure. On one the hand, the official serving the subpoena on Swiss territory can be subject to criminal proceedings and, on the other hand, an employee of a Swiss company responding to it would also incriminate himself.

24. A solution might be to convince the US agency to take back the subpoena or not to enforce it, even though it is not a viable option in every situation. Also, a possible option might be to ask for permission from the Swiss authorities or to just conduct the interviews outside of Switzerland.

25. **S2)** The subpoena not only covers witness testimonies, but also includes a request for documents. Documents could be requested from the company itself, third parties and may even be request for bank statements.

26. The problems and solutions will be the same as in section S1, but being as the possibility of moving abroad to circumvent Swiss regulations is not an option, the emphasis will shift to other informal ways.

27. **S3)** The subpoena is addressed to the US company demanding records located in Switzerland. Would this make a difference from a Swiss/US perspective?

28. As long as the Swiss parental company can act voluntarily and is not threatened by a sanction of any kind, the 271-issue does not come into play.

29. **S4)** What if there is no subpoena, but only an informal request for documents or to talk to Swiss residents on an informal basis?

30. A lot of informal possibilities are available, like the sharing of documents and records or even the meetings to discuss proceedings. However, the finding of facts through interviews could be difficult and would perhaps be better conducted outside of Switzerland.

31. Nevertheless, great care is necessary to make sure to whom the secret belongs, as only the owner has the authority to disclose it.

F. Cross-border privileges

32. At the beginning of her presentation, Mrs Stern pointed out the two basic privileges in cross-border matters and how to identify, use and protect them. The first would be the protection of confidentiality between a lawyer and a client for the purpose of giving or obtaining legal advice. The second one is attached to materials exchanged between a lawyer and a client in connection prior to or during litigation. The range of protection is defined nationally, depending on the details and the context of the communication or materials.

33. To highlight the issues concerning these privileges, three points are to be remembered:

a. Whether a privilege exists or not, often depends on the location or nature of the proceedings. Criminal proceedings may set guidelines different to those in arbitration. Therefore, it is crucial to plan protection according to a whole set of different legal scenarios.

b. It is not possible to rely on the protection of any country involved and therefore it would be negligent not to prepare for its loss.

c. Always prepare material or drafts as carefully as you would prepare unprivileged ones.

34. The attorney client privilege (US) or legal advice privilege (UK) are handled differently in each jurisdiction. For starters, the scope of personal protection is different.

35. For example, an in-house lawyer in Switzerland has no privileged communication, unlike in the US or the UK where they are protected by privileges. But as in-house lawyers often wear several hats, a judge will closely scrutinize the communication in question and forego protection if it does not fall within the scope of the attorney-client privilege.

36. Also, the definition of who the client is can become relevant. When advising a company in the US, the company is the client and not their officers or employees. However, the privilege only applies to the group of those who need to know the information due to their role in giving or those obtaining legal advice. This can also include external experts of any kind that are involved. By contrast, in the UK a small core group inside the company needs to be defined as the client. Disclosure to anyone outside this group, even in order to get case related information is not protected by the legal advice privilege.

37. Although the protected group in the US is larger, disclosing information to an outsider like a regulator, banker or auditor can not only result in the waiver of the privilege related to a document but in the whole subject matter. Contrary to this, in the UK the concept of a limited

waiver exists. It is possible to voluntarily disclose privileged information to a regulator without waiving it in respect of anybody else.

38. There are also differences between the litigation privilege (UK) and work product privilege (US). In the US, the work product doctrine protects the opinions of lawyers and also the so-called normal or ordinary work product. During litigation, an adversary who has substantial need of such a normal work product can go to court and claim it from the company. For example, if one side has got a witness statement and the witness in the meantime has become unavailable. In the UK, the privilege connected to litigation extends to a far larger group. Third parties in- and outside the company can be involved in preparing for the litigation and their material is protected as long as it is produced at the direction of a lawyer.

G. Cyber attacks and necessary precautions

39. As the final presenter on the topic of data protection, Mr Golodner started by speaking about large scale cyber-attacks against infrastructures (e.g. Stuxnet) and companies like Sony Motion Pictures (e.g. DoS and publication of company interna). Such cyber-attacks can turn into physical harm by destroying confidence, diminishing reputation and even blowing up whole factories by disabling control systems (e.g. the explosion of a furnace at a German steel mill). In the case of Sony Motion Pictures, the cyber-attack led to the subsequent dismissal of the CEO and to a 47% loss of income in the fourth quarter of 2014.

40. The size of this informational warfare threat is substantial, as shown by its huge international media coverage. It was named as the primary threat by the US director of national intelligence.

41. It is of top level concern for governments around the world, both as an economic as well as a national security issue. For instance, China and the US set up groups directly advising the PM or President to prevent state or non-state actors bringing down critical infrastructure. Modern states protect themselves by building weapons, but as the critical infrastructure is mostly owned by private companies, the problem has taken on new dimensions.

42. Additionally, the theft of intellectual property has become the largest form of theft in history. A study by Intel Corp estimated the amount of economical and structural damage to innovative countries as being at $400B in 2014.

43. Companies are also directly hit by the theft of intellectual property, customer data and money. This if often not recognized at first, but is only brought to the company's attention when they are informed of it by the enforcement agency.

44. Additionally, there are sometimes non-monetary incentives to attack companies or states. These problems caused by Hacktivists are motivated by their displeasure with the values represented by the attacked entity.

45. Insiders form the fourth group of possible cyber threats to companies. Their incentives range from revenge to personal beliefs and to monetary incentives. Their actions include destruction of data, selective publishing of interna and also include theft of intellectual property.

46. A multitude of precautions should be taken as it should be clear to everybody that there is no such thing as 100% security.

47. The view on those dangers was described as "swirling", for it is regarded differently by national business cultures and therefore, in a multinational company, a core value has to be found. Chasing the problem on a day to day basis would get the company "lost in this vortex." As an example, the value of Cisco was cited as: "driving innovation and security into products and not to regulate the design nationally to move away from a global system and tear apart the interoperability of the internet".

48. Mr Golodner calls the approach that he likes to take "Real Security or Crown Jewel Security." To manage the risk, all departments inside a company have to agree as to which part of the company represents the core value and then to sufficiently protect it. Identifying the adversaries and understanding their motives gives valuable feedback as to the choice of the “Crown Jewels”.

49. Finally, what happens if you are hacked and customer data or intellectual property is stolen? You will have to prove that reasonable care was taken and/or good business judgement was used. To do so, there are different approved methodologies.

50. The message to take home was: A general recommendation to use up to date table top exercises or red teams to think through cyber-attack scenarios. Further, it would be useful to prepare a cross-functional go-team, which will act as first responder in the event of a cyber-attack.

IV. CLOSING REMARKS

51. To conclude the discussion, Mr Länzlinger returned to his raison d'être of panels like this and pointed out once more the fundamental mismatch between the globalisation of business compared to that of the globalisation of law and jurisdictions.

52. Trying to rely on Swiss blocking statutes is like "bringing back the dinosaurs" and will not work for companies doing their business globally. On the other hand, it is absolutely understandable that states try to protect their economy by means of the law.