Privacy in Cross-Border Investigations

International Privacy and Security Forum
Washington, D.C., February 27, 2018

Jaqueline Cooney, Thomas Steiner, Daniel Weber

PAUL HASTINGS

VISCHER

Agenda

I. Current Trends in Cross-Border Investigations
II. Increasing Importance of Internal Investigations
III. Privacy in Cross-Border Investigations
    (1) How privacy issues may constrain multinational corporations' ability to cooperate with foreign authorities
    (2) European Union and Swiss Perspectives
    (3) U.S. Perspective
    (4) Beyond Europe and the U.S.
IV. Takeaways

I. Current Trends in Cross-Border Investigations

Current Trends in Cross-Border Investigations

- DOJ and other authorities focus on (mis-)conduct occurred outside of the U.S.
  - Volkswagen, Swiss Bank Program (80+ Swiss Banks), UBS, Credit Suisse, FIFA, Petrobas, etc.
  - Panama Papers, Paradise Papers, 1MDB
- DOJ is also prosecuting individuals
  - Foreign executives, in the wake of the Yates Memo; example: FIFA and Petrobas executives
- Cooperation is key:
  - High disclosure obligations (in the wake of the Yates Memo, including disclosure of employee names at an early stage) as prerequisite for cooperation credit
  - Establish the relevant facts through an Internal Investigation (e.g. for leniency application/self-reporting)
- Increasing interest in (cross-border) disclosure of employee and client information
  - Business emails, minutes, policies, interviews, report of the Internal Investigation

II. Increasing Importance of Internal Investigations

Increasing Importance for Internal Investigations (1/2)

- Definition: “An Internal Investigation is a systematic, in-depth analysis of facts launched by a corporate entity and conducted by internal or external counsel of the company. The investigation is usually closed by a report and recommendations”
  - Not an internal audit and not a regular compliance review
- Increase of Internal Investigations in the past 10 years
  - Increase of compliance regulations, government investigations in regulatory and criminal law matters and media reports on corporate compliance issues
  - Triggers for Internal Investigations: Suspected breach of regulatory duties, criminal law or internal compliance rules
  - Internal Investigations mandated by regulators (DOJ; Swiss Financial Supervisory Authority) vs. Internal Investigations triggered by a whistleblower or another incident
  - “Duty to investigate”: Boards must know the relevant facts (informed decision-making)

Increasing Importance for Internal Investigations (2/2)

- Life Cycle of an Internal Investigation: (1) Initiation and Planning, (2) Execution, (3) Results
- Uses of personal data regulated by Swiss and EU data protection laws
  - Swiss and EU data protection laws define “processing” of personal data as any operation with personal data. Processing includes, without limitation, the collection, storage, use, revision, disclosure, archiving and destruction of data
  - This definition is broad and includes both the collection and analysis of data in an Internal Investigation and the disclosure of personal data and other data to foreign authorities
  - Comprehensive document collection, document review/interviews, reports during an Internal Investigation
- Complexity of Internal Investigations
  - Several players, legal privilege: Securing information in multiple jurisdictions (information flow)
  - Restrictions on the transfer of (employee and other) personal data from EU/EEA/Switzerland to any country without adequate level of data protection

III. Privacy in Cross-Border Investigations:

How privacy issues may constrain multinational corporations' ability to cooperate with foreign authorities

Privacy Issues in Cross-Border Investigations

- Divergent (local) data privacy and employment laws
- Lawful (local) collection and (cross-border) disclosure
- Balancing interests of the employer and the employee
- Consent: unlikely to be practicable and/or valid
- Information notices vs. confidentiality of cross-border investigations
- Limitations on cross-border data transfers
- Employees' access and deletion rights
- Secrecy, privilege and blocking statutes

III. Privacy in Cross-Border Investigations:

European Union and Swiss Perspectives

Lawful Collection and Disclosure

- Compliance with legal obligation
  - laid down in EU *or* Member State laws, *and*
  - which applies to the company
- Legitimate interest
  - pursued by company (or third party)
  - *overriding* the employee's interests or fundamental rights and freedoms requiring protection of personal data
- Necessary to perform the employment contract
- Employee's freely given consent?

Legitimate and Overriding Interests of Employer

- Necessary (objectively relevant) for the purposes of compliance with foreign laws and regulations which apply to the company, including for the purposes of receiving cooperation credit in cross-border regulatory investigations
- **Balance of interests test:**
  - Importance of cooperation in cross-border investigation vs. employee's interest in his or her personal data not being reviewed, disclosed or transferred
  - Employer's duty of care vs. employee's duty to cooperate in internal or regulatory investigations
  - Take into account: proportionality and subsidiarity (availability of less intrusive measures – including anonymization or pseudonymization), relevance of personal data for the investigation, consequences for company if data is not disclosed (including sanctions, disqualification from receiving cooperation credit), consequences for the employee if data is disclosed (such as being made subject to civil or criminal proceedings)

Consent: Unlikely Practicable and/or Valid

- Employees must have a real choice whether to consent or not
- Imbalance of power and dependency resulting from employer/employee relationship:
  - "Employees *are almost never in a position to freely give, refuse or revoke consent.*"
  - *"[E]mployees can only give free consent in exceptional circumstances, when no consequences at all are connected to acceptance or rejection of an offer. "*

    (WP 29, Opinion 2/2017 On Data Processing at Work, at p. 23)
- Consent to be as easy to withdraw as to give

→ Consent unlikely to be a valid and practicable basis for the transfer of employee data in cross-border investigations

Information Notices under the GDPR

- EU GDPR emphasizes transparency requirement
- Employer's obligation to provide extensive information, including
  - the purposes of processing
  - the legal basis for processing, including any legitimate interests pursued by the employer
  - the recipients or categories of recipients
  - details on safeguards used for cross-border data transfers
  - the existence of access, restriction and deletion rights of the employees
- Concise, intelligible, easily accessible, using clear and plain language
- Notice to be provided when personal data are obtained or at the latest before the data are disclosed to another recipient
- Limited exceptions apply (including exceptions laid down in Member State laws)

Information Notices vs. Confidentiality of Cross-Border Investigations

- Informing the employee (before disclosure) may jeopardize internal or cross-border investigation or prevent company/employer from effectively defending itself in regulatory investigations
- **Serious impairment of objectives** exception (cf. Art. 14(5)(b) GDPR)
- **Member State laws restricting scope of information rights and obligations** (cf. Art. 23 GDPR)
- **Disproportionate effort** exception (cf. Art. 14(5)(b) GDPR)

Serious Impairment of Objectives

- European Union law: Art. 14(5)(b) GDPR
  - Exception applicable where personal data is not obtained from the data subject (common scenario in cross-border investigations)
  - Provision of the information would "nullify the objectives of the processing" (WP 29, Guidelines on Transparency under Regulation 2016/679, at para. 58)
- EU Member State law: German Federal Data Protection Act (German BDSG):
  - § 33(2)(a) of the German BDSG: Provision of the information would impair the establishment, exercise or defense of legal claims
  - § 33(2)(b) of the German BDSG: Provision (by company) of the information would impair criminal law enforcement

Serious Impairment of Objectives (cont'd)

- Draft of revised Swiss Federal Data Protection Act (Swiss d-DSG): Controller may **restrict, defer or refuse** information if providing the information would **frustrate the purpose** of the processing (Art. 18(3)(c) of the Swiss d-DSG)
- **Note:** employers' duty of care still requires **balance of interests test**
- **Best practice:** General information to be provided at the beginning of employment that company may have to disclose company documents bearing employee's name in cross-border investigation and general information to be provided about internal investigations (incl. whistleblowing) proceedings; provide more information once information will no longer impair investigation

Limitations on Cross-Border Data Transfers

- GDPR restricts transfer of personal data to “third countries”
- Derogation for specific situations: transfer necessary
  - for **important reasons of public interest** (Art. 49(1)(d) GDPR; Art. 14(1)(c)(1) of the Swiss d-DSG), or
  - for the **establishment, exercise or defense of legal claims** (Art. 49(1)(e) GDPR; Art. 14(1)(c)(2) of the Swiss d-DSG)
- **Note:** employers' duty of care still requires **balance of interests test**
- Transfer of employee data to the U.S. DOJ in tax-related cross-border investigation / “U.S. Bank Program” – no “overriding” public interest according to extensive case-law under current Swiss Federal Data Protection Act

Other Relevant Issues

- Employees' right of access to personal data processed by employer
  (Swiss Federal Supreme Court: Employee's right to receive a copy of documents bearing the employee's name that the bank has disclosed to the U.S. DOJ in tax-related cross-border investigation)
- Employees' right to request deletion of personal data or restriction of data processing
- Secrecy laws (e.g. Swiss bank customer secrecy)
- Blocking statutes (e.g. Art. 271 of the Swiss Criminal Code)

III. Privacy in Cross-Border Investigations:

U.S. Perspective

Privacy Rights for Workers in the US

No "right to privacy" in the US as established in the EU; however, workers' privacy rights have been established through statutory provisions:

Electronic Communications Privacy Act

- Three titles:
  - ➢Wiretap Act
  - ➢Stored Communications Act
  - ➢"Pen register" provisions

Pen Register/ Trap & Trace

- Outgoing/incoming
- Permissible for **provider** to monitor
- For operating service:
  - ➢To protect "provider's" rights and property;
  - ➢To protect users from abuse or unlawful use;
  - ➢To record initiation/
  - ➢completion of comm to protect from fraudulent, abusive or unlawful use; and
  - ➢With consent of user

Stored Communications Act

- Important for review of stored data
- Two principal exemptions from authorization requirement
  - ➢Consent by one of the parties to the communication
  - ➢"Provider" exemption
- Microsoft v. United States – 2d circuit ruled against allowing a warrant for seizures of data that could result in ex-US data access
- Other courts have found the opposite (See *In re Search Warrant* about a similar Google case)

Wiretap Act

- Not generally relevant to employers as interception
- Must be contemporaneous (in transit)

State dual-consent laws

- Typically apply to eavesdropping or interception, not review of stored communications

Other considerations

- Reasonable expectation of privacy

Access to Social Media

In both the US and the EU, there has been increasing scrutiny of Social Media monitoring requiring transparency and consent:

Electronic Communications Privacy Act

- Imposes limitations on access to stored communications (and interception)
- Limits provider's ability to disclose communications

Subscriber Not Compelled Directly by Statute

- At least one court had upheld orders requiring such consent

Long-standing Issue

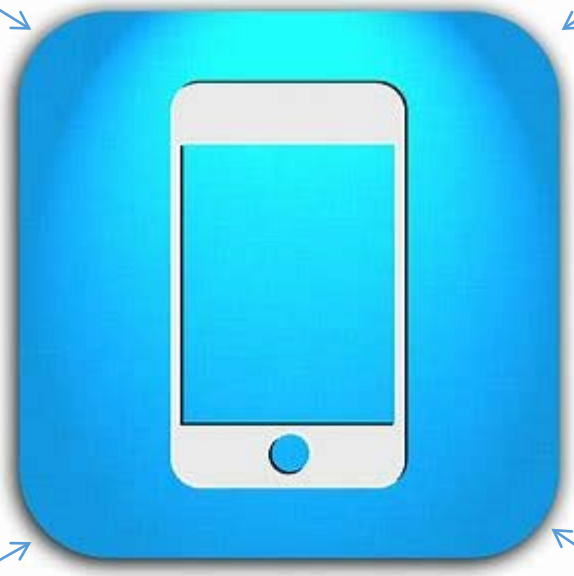
- Municipality in Idaho in interviews of job applicants was first reported incident
- More recently, incident involving correctional authorities in Maryland
- University athletic departments and scholarship athletes (requiring athlete to "friend" a monitor)

Monitoring Mobile Devices in US

BYOD at the workplace has become so common that firms and the government have developed best practices for monitoring devices to protect intellectual property and proprietary data:

What is a reasonable expectation of privacy in an employer/employee setting?

Key is clear communication and limitation of monitoring to work-related reasons



Security and protocols for loss or theft are important considerations

- Remote data wipe capability/segregation of work and personal data

E-discovery challenges

- Personal devices (mobile or otherwise) may be subject to search.

Data Analytics: US vs. EU

User Behavior Analytics in US

- Companies are increasing using sophisticated tools to analyze users' behavior to:
  - Mitigate insider threat
  - To protect personal data and intellectual capital
  - To protect against the inadvertent loss of data
  - To protect against malicious attacks

"Automated Profiling" in the EU

- In the EU, "automated profiling" of data subjects is highly regulated under the GDPR and in some local countries is prohibited or restricted without approval from the local Works Council

Cross-Border Investigations Considerations

- Will the User Behavior Analytics platform (including data loss prevention tools, email scanning tools, and automated monitoring and auditing tools) be used for all employees globally?
  - Often these tools are piloted in the US, so it's important to know where they will be used in a global enterprise
- Have you consulted with your legal department about the local country laws that might affect your use of these tools either for cybersecurity or for investigations?
- Have you consulted with your information security division to determine whether use of the tools can be modified in different jurisdictions?

III. Privacy in Cross-Border Investigations:

Beyond Europe and the U.S.

Asia, Latin America, and Africa/Middle East

- Although focus most recently is on changes in EU privacy law, data protection laws in other areas of the globe continue to grow and change. Generally, these data protection regimes require transparency about the collection and use of personal information:

Asia

- South Korea, Hong Kong and New Zealand require affirmative opt-in consent for some uses of data
- Most countries with data protection laws also require data to be handled securely (See also restrictions in China's new cyber law)
- A number of Asia-Pacific countries restrict cross-border data transfers to countries w/o adequate data protection

Latin America

- All relevant privacy laws include choice requirements
- Colombia has a much stronger emphasis on affirmative consent than other
- Many privacy laws in Latin America rely heavily on consent for cross-border transfers of information

Africa/Middle East

- 18 countries (plus areas in UAE and Qatar) have enacted comprehensive privacy laws, almost all of which include cross-border limitations (exceptions in made cases include transfers based on contractual necessity)

IV. Takeaways

Takeaways

- Data privacy issues may significantly constrain multinational corporations' ability to fully cooperate in cross-border investigations
- Increasing appreciation by U.S. law enforcement authorities of foreign data privacy laws, but company under investigation has to identify all available legal bases to provide information/documents
- Exceptions and derogations available in foreign data privacy laws, but balancing of interest test required
- Data collection is local (although investigations are increasingly global) – important to understand local privacy laws