
PETERS & PETERS

*ELECTRONIC DATA PRESERVATION AND
COLLECTION – A LAWYERS PERSPECTIVE*

ECBA TALLINN 6th OCTOBER 2012

Neil Swift

Partner

nswift@petersandpeters.com

Introduction

- A. Context
- B. Legal Issues
- C. Practical Considerations

When and how does it arise?

- Individuals
 - Pre-investigation
 - Materials not obtained by law enforcement
- Corporate clients
 - Internal investigations
 - Compliance with compulsory powers

Why is it important?

Capturing evidence and preserving its integrity

Documents

- When were they created? By whom?
- Who amended them? When?
- Do different individuals have different versions?
- Have they been deleted? When?

Emails

- Who sent? Who received? When?
- Were they opened? When?
- Were they forwarded?
- Have they been deleted?

Internal Corporate Investigations

- Where the US leads...
- Corporate governance
 - obligations to market
 - perception of investors, counterparties, customers, employees
- Corporate criminal liability
- Follow on liability – Proceeds of Crime Act
- Advantages to self reporting
- Benefit of cooperation
- From crisis to risk management

Regulators

- Regulatory risk – UK
 - Financial Services Authority (FSA) – financial market activity
 - Office of Fair Trading (OFT) – competition law including anti-trust
 - Serious Fraud Office (SFO) – fraud and corruption
 - HM Revenue & Customs (HMRC) – taxes
 - Crown Prosecution Service (CPS) – other crime
 - Department for Business, Enterprise and Regulatory Reform (BERR) – Companies Act
 - Others
- European Commission
- Other national authorities?

Compulsory Powers

- Available to a number of regulators during the course of their investigations
- May arise from own investigation or follow an internal investigation
- Sanctions for non-compliance
 - Contempt of court
 - Criminal offences
 - Justification for warrant
 - Consequences where a duty to cooperate exists (FSA)
- Mutual Legal Assistance

Legal Issues

- Data Protection Directive
- Privilege

Data Protection Directive

- General in its terms
- Imposes minimum standards
- Member states discretion leading to different rules
- Need legal advice in each affected jurisdiction
- UK statute requires fair & lawful processing of personal data
 - Prior consent
 - In pursuit of legitimate interests where no prejudice to privacy of affected individuals
 - Necessary for compliance with non-contractual legal obligation
 - Necessary for administration of justice

Privilege

- Advice privilege, covering confidential communications between client and lawyer
- If investigation in contemplation of litigation, broad range of communications protected by privilege if dominant purpose is for that litigation
- English law protects documents which satisfy English test for privilege, irrespective of how it would be treated in others (including country of origin)

Practical Considerations

- Identifying scope
- Location and lock-down
- Communication
- Suspending destruction
- Collection
- Access and organisation
- Review
- Recording disclosure

Identifying scope

- No general express obligation to retain records for purpose of internal investigation (but obligations exist for other purposes)
- Minimum time periods vary by country
- Extent of obligation governed by sanctions for destruction / disposal
- What is the allegation?
- What is relevant?
- Be conservative
- Keep under review

Location and lock-down

- Involvement of IT staff
- Involvement of operational staff
- Domestically hosted material
- Overseas hosted material
- Multiple physical locations

Communication

- Strong and clear message within business to ensure that users do not alter or delete material
- Does message need to be communicated internationally?
- Be aware (and beware) of IT projects underway
- Ensure clear line of communication with IT

Suspending destruction

- IT staff need to be aware
- Immediate suspension of IT retention / destruction policy
 - Routine destruction of old data
 - Hardware recycling
 - Overwriting back-ups
 - System migration (between countries and between IT systems)

Collection

- Current servers
- Current server back-ups
- Archived systems
- User hard drives – laptop / desktop
- User back-ups
- Portable storage devices
- Smart phones

Access and organisation

- In multi-jurisdictional investigation, who can access what and from where?
- Once collected, need to have a means of organising / collating material

Review

- How to review?
- Search terms?
- Intelligent review / prioritising multiple hits
- Collaborative approach with law enforcement?

Recording disclosure

- Need to know what was disclosed, when and to whom
- Means of recording reasons for non disclosure – e.g. basis for privilege claim

QUESTIONS?