



# (Some) legal aspects of cryptography

Royal Holloway University of London  
December 2005

Robert Carolina

+44 (0)7712 007 095 (mobile / business)

robert.carolina@sciocertus.com (primary - for course questions)  
robert.carolina@origin.co.uk (client enquiries)

---

---

---

---

---

---

---

---

## About the presenter



### • US lawyer & English Solicitor

- University of Dayton (BA, Political Science, 1988)
- Georgetown University (Juris Doctor 1991)
- London School of Economics (LL.M, International Business Law, 1993)
- Senior Visiting Fellow, ISG, Royal Holloway University of London (1997- date)
- Co-editor, Sweet & Maxwell's Encyclopedia of E-Commerce Law (initial release December 2003)

Copyright © Robert Carolina. All rights reserved.

2

---

---

---

---

---

---

---

---

## About Origin



### • Law firm

- Regulated by the Law Society of England & Wales
- Intellectual property specialists

### • Industry focus includes:

- Mobile communications technology
- Banking technology & payment systems
- Information security technology

### • Clients - large and small

Copyright © Robert Carolina. All rights reserved.

3

---

---

---

---

---

---

---

---

## The ground rules

- **Academic freedom**

- Journalists: this is off the record / not for attribution generally
- Comments represent my opinion only

- **NOT legal advice**

- Rules changing rapidly
- Criminal sanctions may apply
- Obtain specific advice before taking action

---

---

---

---

---

---

---

---

## Overview of presentation

- When law “discourages” use of crypto
- Law “encourages” use of crypto?
- Law interferes with “neat” crypto ideas
- Digital signatures and liability
- The E-Signature Directive and UK transposition
- Problems in cross-border e-signatures

---

---

---

---

---

---

---

---

## “Values” supported by crypto

- **Authentication**
- **Confidentiality**
- **Integrity**

---

---

---

---

---

---

---

---

## Intersection: cryptographic technology and law



- Law discourages applications
- Law encourages applications
- Law interferes with a “neat” idea

Copyright © Robert Carolina. All rights reserved.

7

---

---

---

---

---

---

---

---

## When law “discourages” use of crypto



When law “discourages” use of crypto

---

---

---

---

---

---

---

---

## Law discourages use



- Export restrictions
- Import restrictions
- Use restrictions
- Intellectual property rights
- [Trusted third party regulation?]

Copyright © Robert Carolina. All rights reserved.

9

---

---

---

---

---

---

---

---

## Export restrictions

- **“Movement” of the technology itself**
  - Licence required?
  - Exception applicable?
- **Not just USA**
- **Re-export restrictions**
  - “Extraterritorial” regulation
  - Requirement on exporter to impose contract restrictions on end-user

---

---

---

---

---

---

---

---

## Export restrictions

- **Financial services applications**
  - Historically given an easy ride
  - Requirements to immobilise the black box
- **“Dual use” goods**

---

---

---

---

---

---

---

---

## Import and Use restrictions

- **Import restrictions (opposite of export)**
  - Licence required?
- **Use restrictions**
  - The most famous are France and Russia
  - France has liberalised significantly

---

---

---

---

---

---

---

---

## Move to intangibles

- **Most regulation assumed tangible technology**
- **Laws of US and others - clearly apply to intangibles**
  - Export “events” can include lectures to foreign nationals which take place within the territorial US
  - Equally, can apply to lectures to foreign nationals which take place outside the territorial US

---

---

---

---

---

---

---

---

## Move to intangibles

- **Intangibles “loophole”?**
  - Sometime the law applies only to “goods”
  - UK government recently broadened focus of statute
  - Caution: extremely dangerous to rely upon this exception - if you get one thing wrong it is a criminal offence
- **Financial applications**
  - No longer an easy ride for many

---

---

---

---

---

---

---

---

## Move to intangibles

- **US First Amendment litigation the (basic) argument:**
  - Software is a type of “expression”
  - Expression is a type of “speech”
  - Ergo, export restriction is a “prior restraint” on speech
  - Prior restraint only appropriate in the most narrow of circumstances (as per the US Constitution)
  - Export rules on source code are overly vague and thus unconstitutional

---

---

---

---

---

---

---

---

## Move to intangibles

origin

- **Bernstein vs US Dept of State**
  - Bernstein is a mathematician seeking to “discuss” his work with colleagues internationally
- **US District Court (ND California)**
  - Decision 25 August 1997: (1) source code IS speech, (2) export regs are improper prior restraint (safeguards “woefully inadequate”)
- **Appealed. US Ct Appeal 9th Circuit**
  - Argument on 8 December 1997

Copyright © Robert Carolina. All rights reserved.

16

---

---

---

---

---

---

---

---

## Move to intangibles

origin

- **Junger vs Daly (Dept of Commerce)**
  - Junger is a law professor in Cleveland, Ohio; occasionally dabbles in cryptographic software
- **US District Court (ND Ohio)**
  - Decision 2 July 1998: source code IS NOT speech; it is “inherently functional”
  - Rejects rationale of the Bernstein trial court decision
- **Appealed. US Ct Appeal 6th Circuit.**

Copyright © Robert Carolina. All rights reserved.

17

---

---

---

---

---

---

---

---

## Move to intangibles

origin

- **Bernstein Appeal: A decision!**
  - 9th Circuit issues opinion on 6 May 1999
  - Source code “is expressive” (appears to reject the “inherently functional” argument)
    - but perhaps object code is not
  - Licensing scheme lacks adequate safeguards
- **Motion for rehearing, or rehearing en banc**
  - Asking same court to reconsider
  - VERY rarely granted

Copyright © Robert Carolina. All rights reserved.

18

---

---

---

---

---

---

---

---

## Move to intangibles



- **Bernstein appeal: motion for rehearing en banc granted in October 1999!**

- Decision suspended pending rehearing
- Would be heard before entire group of 21 judges of the 9th Circuit
- Rehearing en banc was set for March 2000

- **January 2000: export rules change**

- Bernstein files motion to remand to District Court

---

---

---

---

---

---

---

---

## Move to intangibles



- **Junger Appeal: A decision!**

- 6th Circuit issues opinion on 4 April 2000
- 'The Supreme Court has explained that "all ideas having even the slightest redeeming social importance," including those concerning "the advancement of truth, science, morality, and arts" have the full protection of the First Amendment'
- This includes artwork, music, and poetry
- Compare sheet music: not everyone can read it

---

---

---

---

---

---

---

---

## Move to intangibles



- **Junger Appeal: A decision!**

- "Because computer source code is an expressive means for the exchange of information and ideas about computer programming, we hold that it is protected by the First Amendment"
- Case reversed and remanded

---

---

---

---

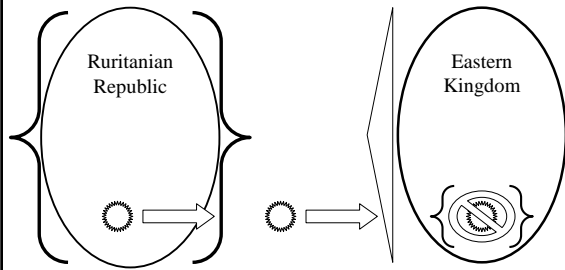
---

---

---

---

## Export/import/use graphic summary



---

---

---

---

---

---

---

---

## International co-operation?

- **COCOM (ends 1994)**

- Semi-formal club of governments to prevent leakage of sensitive technology from “West” to “East”
- Replaced by Wassenaar 1995
- Focus is clearly on technology as a “dangerous” product

---

---

---

---

---

---

---

---

## International co-operation?

- **Council of Europe Recommendation 95(13)**

- **Point No 14:**

- “Measures should be considered to minimise the negative effects of the use of cryptography on the investigation of criminal offenses, without affecting its legitimate use more than is strictly necessary”

---

---

---

---

---

---

---

---

## International co-operation?

- **OECD guidelines promulgated 1997**
  - 8 guiding principles
  - Legitimate commercial use now clearly on the international agenda
- **All examples of “public” international law**
  - Not always self-executing as domestic law
  - Many countries must modify their own rules

---

---

---

---

---

---

---

---

## Intellectual property

- **Patents**
  - Processes (including certain software implementations)
  - National coverage only; no international recognition; must apply in each country where protection is desired
- **Copyright**
  - “Literary works” such as software
  - International recognition by treaty

---

---

---

---

---

---

---

---

## Case study: PGP

- **Encryption software process**
  - Allegedly infringed PKP US patent
  - Therefore could not manufacturer distribute sell or use in the US without an agreement with PKP
- **Strong cryptographic technology**
  - Caught by US export restrictions
  - Therefore could not move software outside of the US without government export licence

---

---

---

---

---

---

---

---

## Case study: PGP

- **Software “appears” outside of the US**
  - PKP could not stop use - patent applies in US only
  - US government slow to react
- **Announcement of PKP licence deal**
- **US Grand Jury investigation announced**
  - No direct evidence of export
  - Ultimately not pursued

---

---

---

---

---

---

---

---

## Case Study: International consumer e-banking project

- **Bespoke software module given to customers to super-encrypt traffic**
- **This client’s risk decision**
  - Overcome the US export hurdle
  - Focus on clearing import and use hurdles for customer’s home jurisdiction
  - Contractual warning about legal restrictions on movement of the technology + customer’s agreement to comply with the law
    - BUT will Customer end up in jail somewhere?

---

---

---

---

---

---

---

---

Law “encourages”  
use of crypto?

---

---

---

---

---

---

---

---

## Law encourages use

origin

- **Private contract requirements**

- Some bilateral and multilateral EDI agreements require use of cryptographic technology

- **UCC § 4A: Electronic Payments (USA)**

- Payment order is “authorised” only if the person actually authorised the order (UCC § 4A-202(a))
- BUT bank may place reliance upon orders issued with a “security procedure” if it is “a commercially reasonable method of providing security against unauthorized payment orders” (UCC § 4A-202(b))

Copyright © Robert Carolina. All rights reserved.

31

---

---

---

---

---

---

---

---

## What is “commercially reasonable”?

origin

- **UCC § 4A-202(c):**

- “Commercial reasonableness of a security procedure is a question of law to be determined by considering the wishes of the customer expressed to the bank, the circumstances of the customer known to the bank, including the size, type, and frequency of payment orders normally issued by the customer to the bank, alternative security procedures offered to the customer, and security procedures in general use by customers and receiving banks similarly situated.”

Copyright © Robert Carolina. All rights reserved.

32

---

---

---

---

---

---

---

---

## What is “commercially reasonable”?

origin

- **TJ Hooper**

- US court case decided in 1932
- Tugboat without a radio caught in storm just off coast; entire cargo barge lost
- If radio had been installed, would not have put to sea

- **Negligence?**

- Would a “reasonable person similarly situated”?
- Most other tugboat companies had not installed radios as they were new and expensive technology

Copyright © Robert Carolina. All rights reserved.

33

---

---

---

---

---

---

---

---

## What is “commercially reasonable”?

- **TJ Hooper Decision:**

- “If  $B < PL$  then negligence”
  - B = cost to implement technological fix
  - P = probability of loss without the technology
  - L = probable amount of loss

- **Conclusions?**

- Ninety-five percent of the people CAN be wrong
- Possible for an entire industry to be negligent even using “industry-standard” practice

---

---

---

---

---

---

---

---

## Use crypto to “enforce” other rights?

- **Does law encourage use of cryptography to enforce legal rights?**

- **Copyright laws**

- Change in focus of copyright law
- The Russian developer case (US)

- **Law of confidential information**

- The Mars case (UK)

---

---

---

---

---

---

---

---

Law interferes with “neat” crypto ideas

---

---

---

---

---

---

---

---

## Law interferes with “neat” ideas

- **Requirements of form**
  - “Signature” and “writing” requirements
  - Other specifications about presentation
- **Evidence problems**
  - The “hearsay” rule
  - The “best evidence” rule
  - Computer evidence rules
- **Digital “money”**

---

---

---

---

---

---

---

---

## Requirements of form

- **Definition (approximate):**
  - Any legal or regulatory requirement that a communication take place in a certain form
- **Examples**
  - UK: “A contract for the sale ... of ... land can only be made in writing and only by incorporating all the terms which the parties have expressly agreed in one document”
  - US: a contract for the sale of goods for a price > \$500 must be in “writing” and “signed”

---

---

---

---

---

---

---

---

## Digital signature law What is out there?

- Utah Digital Signature Statute (1995)
- ABA Digital Signature Guidelines (1996)
- Many other US States followed
- UNCITRAL Model Law (1996)
- German and Italian laws
- EU: Directive on a common framework for electronic signatures (1999)
- UK Electronic Communications Act and follow-up legislation (2000, 2001, 2002, 2003, + ???)

---

---

---

---

---

---

---

---

## Digital signature law What might they do?

- **Provide legal definition of “digital signature”**
- **Satisfy requirements of form**
  - Digital signature is a signature for all legal purposes
  - Digitally signed file is “writing” for all legal purposes

---

---

---

---

---

---

---

---

## Digital signature law What might they do?

- **Establish “standards of care”**
  - Explain how liability is apportioned
  - Provide guidance to each of the players in the digital signature game
  - Provide “safe harbour” to CA

---

---

---

---

---

---

---

---

## Satisfy requirements of form

- **The “shotgun” approach**
  - Single statute with simple statement providing legal equivalence for digital signatures and electronic files that are signed
  - Simple, and relatively easy to draft the law, but may have unpredictable consequences
- **The “surgical” approach**
  - Modify each and every law on the books which contains a requirement of form
  - But the UK alone has more than 400!

---

---

---

---

---

---

---

---

# Digital signatures and liability

## A brief introduction

---

---

---

---

---

---

---

---

## Digital signature - liability

### • Introduction to the players

- Subscriber / Signatory (S)
- Certificate authority / Registration Authority / Certificate Issuer (CA/RA/CI)
  - Assume combined CA/RA/CI model for this part of the discussion
  - We will need to reconsider re ID-PKC
- Third party relying upon signature (TPR)

---

---

---

---

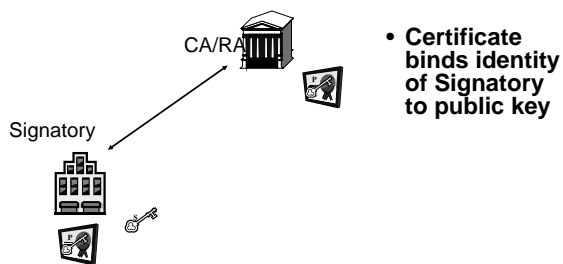
---

---

---

---

## Registration process



---

---

---

---

---

---

---

---



## CA/RA liability?

- **What if CA/RA/CI misidentifies S?**
- **TPR relies upon incorrect certificate**
  - CA/RA/CI duty of care to TPR?
  - CA/RA/CI contract duty to TPR?  
(Is certificate “goods” or services?)
- **Can CA/RA/CI limit liability by contract?**

---

---

---

---

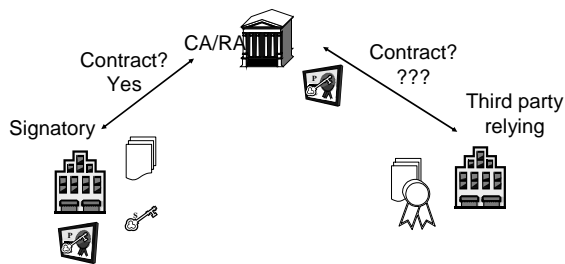
---

---

---

---

## Liability limitation



---

---

---

---

---

---

---

---

## Signatory liability?

- **Maintain control over signature (secret key)**
- **What if it is “stolen”?**
  - For “thief”: is it possible to “steal” a number?
    - English law - No
    - ABA Guidelines - Yes
  - Does S remain liable to TPR?

---

---

---

---

---

---

---

---

# The E-Signature Directive and UK transposition



---

---

---

---

---

---

---

---

## Directive Form issues



### • Signature recognition

- Art 5(1): Member State MUST provide legal equivalence to an e-signature that is
  - An an Advanced Electronic Signature (AES); and
  - Based on a Qualified Certificate (QC); and
  - Created with a Secure Signature Creation Device (SSCD)
- Art 5(2): e-signature may NOT be denied legal effectiveness solely on the grounds that it is in electronic form

Copyright © Robert Carolina. All rights reserved.

53

---

---

---

---

---

---

---

---

## Directive Form issues - UK



### • Electronic Communications Act 2000

- Addresses evidence point (S.7)
- Sets out a **process** to address other issues (S.8)

### • Fails (in my opinion) to:

- mandate recognition of all AES based on QC created with SSCD - Art 5(1)
- remove denial on basis of electronic form - Art 5(2)

Copyright © Robert Carolina. All rights reserved.

54

---

---

---

---

---

---

---

---

## Directive Liability

### • CI liability

- Imposes standard of care on issuance of QC's - art 6(1)&(2) (this is a TPR "sword")
  - Shifts burden of proof - CI must prove it was NOT negligent
- Scope of use limit (art 6(3)) & reliance limit (art 6(4)) for QC's (this is the CI "shield")
  - Limit must be "recognisable" to TPR
- All without prejudice to consumer protection rules (!)

---

---

---

---

---

---

---

---

## Directive Liability - UK transposition

- **Electronic Communications Act 2000**
  - Failed to address liability issues
- **The Electronic Signatures Regulations 2002**
  - Makes a clear statement that TPR has a liability "sword"
  - But FAILS (in my opinion) to assure that CI has a liability "shield"

---

---

---

---

---

---

---

---

## Impact of legislation?

- **Very few "carrots"**
  - ECA S.8 orders are not happening very fast
- **Perhaps a new "stick"?**
  - VAT Directive on e-invoicing (2001/115, 20 Dec 2001)
  - Forces member state taxing authorities to allow e-invoices BUT ONLY if integrity demonstrated:
    - From an EDI system; or
    - Using an "AES" (optional: based on QC and/or generated using a SSCD)

---

---

---

---

---

---

---

---

# Problems in cross-border e-signatures

---

---

---

---

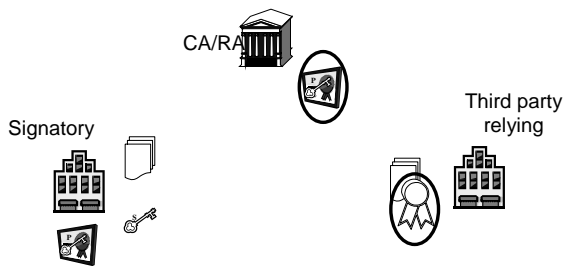
---

---

---

---

## Cross-border recognition



Copyright © Robert Carolina. All rights reserved.

59

---

---

---

---

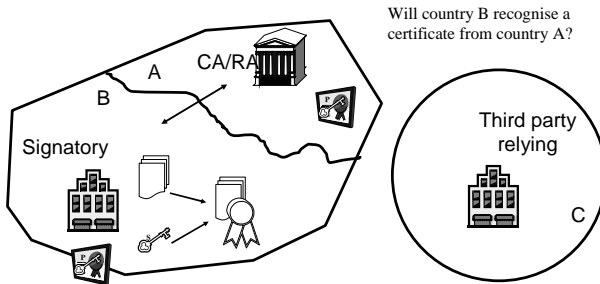
---

---

---

---

## Cross-border certificate



Copyright © Robert Carolina. All rights reserved.

60

---

---

---

---

---

---

---

---

## Recognition of certificates

- **From within EU**

- E-signature directive at art 4
- National treatment principle

---

---

---

---

---

---

---

---

## Recognition of certificates

- **From outside EU**

- E-signature directive at art 7
- Qualified certificates ONLY, and ONLY IF:
  - CA joins national voluntary accreditation scheme; or
  - An EU CA guarantees the non-EU CA; or
  - Recognised by EU Treaty

---

---

---

---

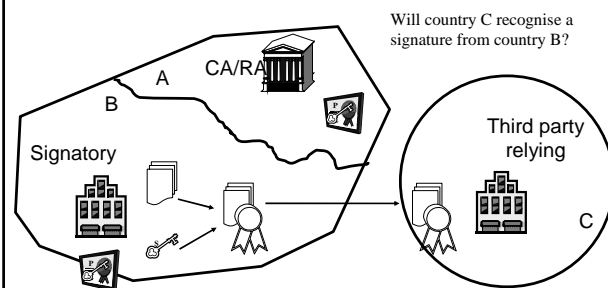
---

---

---

---

## Cross-border signature



---

---

---

---

---

---

---

---

## Recognition of signatures

- **Existing law will sometime recognise “foreign” electronic signatures**

- Example: Rome Convention on Contracts Applicable Law - Art 9

---

---

---

---

---

---

---

---

## Recognition of signatures

- **Rome Convention Article 9**

- Whether non-consumer contract is “formally valid” measured by it’s “applicable law” OR place of either contracting party
- If using agents, place of agent counts

---

---

---

---

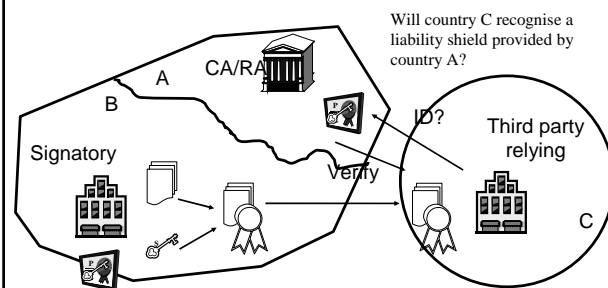
---

---

---

---

## Cross-border CA liability



---

---

---

---

---

---

---

---

## Recognition of liability limit

- **Liability may arise under law of TPR's residence**

- If TPR in EU, article 6 of e-signature directive should help
- If TPR outside of EU, then CA's e-signature directive liability shield may fall away - or simply not exist

---

---

---

---

---

---

---

---

## Digital signature conclusions

- **New laws are weak on cross-border recognition issues**
- **“Closed contract” PKI systems may be best mechanism for rationalising legal risk in the medium-term**

---

---

---

---

---

---

---

---

## Digital money

- **What is “cash”?**
  - What is legal tender?
  - What is debt?
  - What is a deposit?
- **Where is “money”?**
  - Libyan Arab Bank cases

---

---

---

---

---

---

---

---

# Legal Notice



**These materials, together with any training or discussion accompanying the materials provided by the author ("Training"), are intended only to facilitate discussion about issues and do not constitute the provision of legal or accounting advice. Seek professional advice as appropriate. Robert Carolina's services as a practicing lawyer can be obtained from Origin Ltd. (solicitors).**

This presentation is copyright © Robert Carolina. All rights reserved. Robert Carolina asserts all moral rights pursuant to the Copyright Designs and Patents Act. Persons who participated directly in Training and who have lawfully received a copy of these materials ("participant") may redistribute this presentation to additional persons ("recipients") solely in accordance with the following conditions: (i) the presentation is redistributed in its entirety without alteration, (ii) all text logos names contact details and other content must remain unaltered un-obscured and easily seen by recipients, (iii) no charge is made for such redistribution, (iv) there is no attempt to create an impression or otherwise allow an impression to arise that the presentation is the product of any person other than the author, and (v) each recipient must be a member of the same firm or government agency where the participant was engaged in work, or a student in the same school at which the participant was engaged in study, at the time the participant participated in the Training. The Sciocertus name and any related marks are the property of Robert Carolina. Other marks remain the property of their respective proprietors. No rights claimed with respect to government publications including legislation.

---

---

---

---

---

---

---

---

---

---