



IP Policy and Practice Seminar 2005 – Case study:

Episode 2 – NCrypt and the Scamguard Affair

Guidance for participation in the Case Study

The Case Study consists of 5 numbered fact 'Scenarios'. The Scenarios consist of an unfolding sequence of events, mainly relating to your time at DoCIA working on a project called 'SCAMGuard'. Each Scenario will raise a range of IP issues. You are asked to identify and discuss those IP issues.

Please read the Scenarios carefully, reading between the lines as appropriate. Sometimes the issues are obvious; sometime less obvious.

Please confine yourself mainly to IP issues. You may see issues in other areas, eg privacy, procurement, probity, etc. You may note these issues, but the main focus should be on IP.

Each Syndicate will be assisted by a Facilitator. The Facilitator may occasionally steer discussion towards issues, and will be responsible for monitoring time. You have 18 minutes on average to discuss each Scenario (suggested timing is given in the heading for each Scenario).

It is *not* the role of Facilitators to fill in any gaps that you may detect in the fact Scenario, or to expound the law. Note down what needs to be explored, and why. As appropriate make plausible assumptions to enable discussion to proceed. Identifying the questions to ask is more important than knowing all the answers. In some cases the answers will emerge in later Scenarios, or at the end.

The facts described in this case study are fictional and any resemblance to individual agencies or persons is coincidental. The legal issues are, however, real.

Case Study by Philip Crisp - © Australian Government Solicitor 2005.

This material may be used under the terms of the 'Free for Education' licence (click on the logo below for details).



The material is primarily designed for presentation, rather than to be merely read. Inquiries re conducting the Case Study may be directed to philip.crisp@ags.gov.au.

The material does not constitute legal advice. For any important matter you should obtain appropriate professional advice relevant to your circumstances. The facts described in the Case Study are fictional and any resemblance to individual agencies or persons is coincidental. The legal issues are, however, real.

Setting

By the year 2008 the twin problems of spam and internet scams had become such a nuisance that they were seriously impeding the development of E-commerce. Governments all around the world were looking for solutions. After it was elected to office for the sixth time, the Howard Government created the *Department of Communications Infrastructure and the Arts (DoCIA)*, largely in order to provide a more focussed response to the spam/scam menace.

Dramatis Personae

- **DoCIA**: the Department of Communications Infrastructure and the Arts.¹
- **You**: you've just joined DoCIA as their *Assistant Director - IP Commercialisation*. In your early days you learnt all about franchising by helping develop a business strategy for a donut and coffee chain. This was followed by a stint on the 'Mediwise' smartcard project.² You had a short but stellar career on 'The Block' before you were evicted under dramatic circumstances; but landed on your feet by scoring a plum job advising Channel Nine on character merchandising deals with the other contestants. On top of that (so your CV states) you 'featured' in an AGS seminar on IP! You therefore come highly recommended as a person with exactly the broad experience required for the job.
- **Bruce**: your boss. In fact it was Bruce who recommended you to DoCIA. He was your boss previously on the *Mediwise* project, but neither of you talk about that much. After a short political career he has joined DoCIA as *Director - Business Strategies*.
- **NCrypt Pty Limited**: The company engaged to develop the SCAMGuard system.
- **Delia**: CEO of NCrypt Pty Limited.
- **Klaus**: young, middle level IT officer in DoCIA assigned to work with NCrypt. The real brains behind the SCAMGuard technology. Dresses gothic. Dedicated blogger. He is currently writing a paper on advanced data mining techniques to be published in the *Pacific Journal of Heuristic Computing*.
- **Meredith**: Ancient treasure. Has been in DoCIA in five previous incarnations (of the Department, not Meredith as is sometimes unkindly suggested). She is the repository of much corporate knowledge. She says Chip tends to ask hard questions that no-one thought needed to be answered.
- **Chip**: your external legal advisor (of last resort).
- **ACAT**: the Australian Centre of Arts and Technology - introduced in Scenario 4.

¹ DoCIA is an FMA Act Agency, if anyone is wondering.

² Actually that failed so spectacularly that it became an AGS Case Study.

1. Introducing SCAMGuard (25 minutes)

DoCIA commissioned NCrypt Pty Ltd to work on technology to neutralise spam and internet scam messages within the Australian government's internal communications network. The Contract provides that IP in the 'Contract Material' vests in the Commonwealth 'as represented by DoCIA'. This does not apply, however, to any modules previously developed by NCrypt or acquired from a third party. In relation to such modules DoCIA enjoys a licence only, to use the IP for 'the services of the Commonwealth'.

The solution developed by NCrypt proved to have far wider application than previously expected. Although it was not part of the specifications in the Contract, NCrypt developed a new metadata standard and associated functionality, which are implemented in a module called 'Mapper'. This extends the capability of the system so that it can easily be applied on the open internet. To achieve that, the Mapper module must be downloaded and installed by the owners of file servers involved in routing internet traffic, including the main hub-servers and ordinary ISPs.

The core of the system, however, is a secret algorithm³ called (for some reason) '*Inference Engine No.9*' (IE9) which resides on the DoCIA mainframe. Working together with file servers that have installed Mapper, it uses data mining and heuristic⁴ techniques to:

- detect spam and internet scam emails;
- quarantine them on internet hub servers and ISPs *before* they propagate through the internet system;
- apply active counter-measures to confuse and disable the senders.

The technology is considered quite revolutionary. In delivering the completed system Delia mentions proudly that the IE9 module applies a similar approach to that utilised in the Google search engine. DoCIA has tentatively named the system 'SCAMGuard'.

Your task is to consider the circumstances described, identify the possible forms of IP in SCAMGuard, and undertake a SWOT⁵ analysis with a view to promoting its adoption within the Commonwealth, and more widely.

Possible forms of IP

Strengths

³ Although the term 'algorithm' is used in different senses, we are using it here to mean a series of logical steps to be performed (usually, as here, on a computer) to achieve a particular result. In that sense an algorithm may be seen as an abstraction, distinguishable from the particular statements or code in which it may be expressed.

⁴ The term 'heuristic' here refers to the property of a computer system that is programmed to learn from its experiences. Heuristic techniques are often used in various forms of 'artificial intelligence' system.

⁵ that is: analyse the strengths, weaknesses, opportunities and threats in our position.

Weaknesses

Opportunities

Threats

2. A business opportunity emerges (15 minutes)

Bruce calls you into his office. On arriving you discover Bruce, Klaus and Delia are in animated discussion about the prospects for commercialising SCAMGuard. Delia says that she has been in discussion with telecommunications authorities in New Zealand and several Asian countries (which she can't name) about implementing the system in their jurisdictions. She tables a 10-page document described as: 'NCrypt Proposal to DoCIA - SCAMGuard Business Plan'. The Plan incorporates projections of revenue and royalties that would be payable to DoCIA.

After Delia leaves you ask Bruce why we are entertaining proposals for commercialisation from NCrypt at this stage, without testing the market. You don't recall anything in the Contract about NCrypt having rights to commercialise the system. In fact the Contract provides that they were to deliver up all copies of the source code, and they had continuing obligations to protect DoCIA's 'confidential information' which is identified in the Schedule as including 'all source code'.

Bruce replies that the original RFT (from which NCrypt was selected) had a section on 'Commercialisation', foreshadowing that DoCIA would be interested in exploring the prospects of a 'partnering' arrangement with the successful tenderer. He says this is required under 'government policy' which seeks to avoid 'locking up' the Commonwealth's IP. However as the Contract was put in place in rather a hurry there was no time to include any 'Distributorship' arrangements. So it was left to be worked out later.

Any observations on Contract management?

What might be involved in a 'partnering' arrangement?

Is Bruce right about the policy?

Should we commercialise now with NCrypt?

3. Commercialisation options examined (20 minutes)

Despite your reservations, Bruce has decided that he wants you to move *post haste* to bring the benefits of SCAMGuard to the world. He wants to avoid a further selection process, and thinks we can work well with NCrypt.

However you are concerned about the need for a proper evaluation of the options, and you consult Chip urgently. You describe the SCAMGuard project over the phone. You inform him that the pre-existing modules we had been concerned about are very minor, and easily able to be re-engineered if necessary. Based on your telephone description of the system he sends you an email setting out briefly a number of possible options:

- 1) DoCIA could commercialise the SCAMGuard system itself.
- 2) Call tenders for the sale of DoCIA's IP rights in the system.
- 3) Issue a Request for Proposals (RFP) from firms interested in commercialising the system, leaving it up to bidders to spell out their preferred commercialisation model.
- 4) Appoint NCrypt as Distributor on the basis that royalties (paid to DoCIA) would be calculated as a percentage of all revenue from commercialisation.
- 5) Appoint NCrypt as Distributor on the basis that royalties would be calculated as a fixed dollar amount for each 'sale'.

Chip's email finishes with the remarks:

These are just very brief options and I haven't had time to explore the advantages and disadvantages of each. I am in the throes of preparing for a seminar right now. I'll check with you later about this. In particular there may be some other options that we could explore, but I'd suggest we could best do that in a meeting.

Regards, etc.

Over the next week you ponder the advantages and disadvantages of each option.

1. DIY option

2. Sell option

3. RFP option

4. **Appoint NCrypt - Royalties based on a percentage of revenue**

5. **Appoint NCrypt - Royalties based on a fixed dollar amount for each 'sale'**

6. **What other issues or options can you see?**

4. Secondment to ACAT (15 minutes)

In addition to its mission of combating spam and internet scams, DoCIA has responsibility for the arts. Following an election commitment, they participate in establishing the Australian Centre of Arts and Technology (**ACAT**). This is described in the Annual report as a 'joint venture' between DoCIA and the National Gallery of Victoria. ACAT seeks to record and promote synergies between the arts and sciences, with a particular focus on how Australian art has evolved through the use of new technologies. ACAT is headquartered, and maintains its collection, in Albury.

A week after the conversation in Bruce's office you are 'seconded' to ACAT. That is a posting you had not asked for and did not expect. But it suits anyway because it will generate material for your Masters thesis: '*Cultural Aspects of Australian Small Enterprise 1950-2000*'. The ACAT Centre is full of relevant historical material, and the curator is known as a walking repository of oral history.

Your role will be to manage all licensing issues in relation to collection items. The previous occupant was quite disorganised and didn't know (it was said) a warranty from an indemnity.

The curator consults you about a proposal to use self-operated kiosks in various locations in the Centre to guide visitors, as the budget for employing staff is limited. The kiosks will feature black and white footage from old Australian newsreels (up to the early 1950s), showing people using or demonstrating icons of Australian enterprise and technology, such as the Hills Hoist and the Victa lawnmower. The original sound track is to be replaced with voice-overs (with simulated hissing sound) in which the people can be heard directing visitors to relevant displays. The footage was sourced by your predecessor from a commercial film library. The transaction is constituted by emails, phone conversations, a catalog entry and an invoice which refers to a 'Sale - Access stock images from archive @ 600bpi - Total fees: \$2570', followed by a series of catalog numbers in the form: '000211958.mpg'.

You wonder whether the copyright in the film footage has expired. At the AGS IP Seminar last year you learned that copyright in a film lasts for 50 years after the year of publication, so apparently it's out of copyright. You ask Chip to confirm this. 'Yeah . . .', he says, '. . . tricky! I'll get back to you.'

You receive a string of emails from Chip:

Email #1: *The 50 year term is not correct any more. Following the US FTA amendments the term for films has been extended to 70 years from the year of first distribution (s.94). The footage is still in copyright. Best wishes for the project, Chip.*

Email #2: *Sorry; I was mistaken! The US FTA amendments did not revive expired copyright. The film footage would therefore have run out of copyright 50 years after it was first distributed, which would be a year or two ago. Regards, Chip.*

Email #3: *I've looked at it again. As the film was made prior to the commencement of the 1968 Act, the duration of copyright is governed by the transitional provisions in Part XI of the Act. Section 221 says that copyright does not subsist in a film made prior to commencement of the Act. You might think from this that it never was in copyright. However, s.222 says (I am simplifying here) that copyright subsists in **each frame** constituting a pre-1969 film, **as if it was a photograph**. Under s.33(2) copyright in a work (including an artistic work, which includes a photograph) lasts for the life of the maker plus 70 years. The film footage is still under copyright. I told you it was tricky! All the best, Chip.*

Issues arising from the 'secondment' to ACAT

What issues arise from our use of the film footage?

What simple lessons (about copyright duration) do you glean from Chip's emails?

If the film footage is still in copyright, do we have a licence to use it?

Could the 'voice over' infringe moral rights in the film footage?

What other issues can you see?

5. Homecoming surprises (15 minutes)

The secondment to ACAT is twice extended. When you return to DoCIA a year later, you discover that NCrypt has been appointed a Distributor, under an arrangement whereby they are to pay a 10% royalty to DoCIA on net sales of 'Product'. You note some aspects of the royalty provisions that are questionable, but one that really catches your eye is a clause stating:

Ownership of any new modules developed by Licensee⁶ and included in Product shall vest in Licensor⁷ where Licensor elects to fund such development by foregoing royalties.

Other aspects of the Distributorship Agreement seem to assume that future development work will occur within DoCIA: for example, there is a clause requiring the Licensor to 'keep the Licensee informed' of any new versions. There is also a clause stating that the Licensee does not have and will not take a financial interest in any competitive product to *the* Product.

The file contains a note which reads:

Delia called from Auckland airport. Two new modules developed to enable sale to NZ to go ahead. DoCIA can retain full ownership but cost of development to be offset against royalties. Agree (in principle). To be formalised in contract variation.

Meredith, please consult Chip about this.

(Sgd) Bruce

Meredith says she did not see the note. In any event no royalties have been received from NCrypt, although they were required to report every 6 months. Chip says his copy of the Agreement does not include the 'royalty offsets' clause. Meredith says the clause was added (without obtaining legal advice) in last-minute negotiations prior to signing of the Agreement.

You note that the Agreement includes the following clause:

The Distributorship shall continue for a Term of 10 years and thereafter from year to year unless terminated by 3 months' notice from the Licensor (DoCIA) to the Distributor.

Your thoughts on how this has been managed (if printable)?

What action might be taken to clarify DoCIA ownership and entitlement to royalties?

Do you have the right to terminate the Distributorship Agreement?

⁶ NCrypt

⁷ DoCIA

