



*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 in the 'Answers' version of the Case Study to be distributed at the end of the Seminar.

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](mailto: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.<sup>1</sup>
- **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.<sup>2</sup> 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.

**[NOTE:** The Case Study is designed to be conducted for participants who have read the AGS *Outline of Intellectual Property Law*, or who otherwise have some familiarity with IP. The 'Answers' version includes a Schedule with an index of IP concepts addressed in the Case Study.]

---

<sup>1</sup> DoCIA is an FMA Act Agency, if anyone is wondering.

<sup>2</sup> 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 algorithm<sup>3</sup> 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 heuristic<sup>4</sup> 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 SWOT<sup>5</sup> analysis with a view to promoting its adoption within the Commonwealth, and more widely.

---

### Possible forms of IP

- The computer code is protected under *copyright* as a 'literary work'.
- The name 'SCAMGuard' may be registrable as a *trade mark*. However the name 'IE9' might involve some confusion with MS Internet Explorer.
- There may be some *confidential information*, especially in connection with the IE9 algorithm.
- If the algorithm is novel and incorporates an 'inventive step' it may be proper subject matter for a *patent* application. A patent attorney could advise on that.
- In addition, *copyright* may subsist in the specification or template for the metadata standard.
- A *certification trade mark* could be developed to 'certify' the hub servers and ISPs who implement the standard by installing the Mapper component.

---

<sup>3</sup> 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.

<sup>4</sup> 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.

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

## Strengths

- *Copyright*: The original SCAMGuard code written under the Contract (i.e. 'foreground IP') is probably owned by DoCIA. [To be absolutely sure, you might need to check that the Mapper module which enables the system to be applied on the open internet *is* part of the 'Contract Material' - given that it implements functionality that was not 'specified'. The answer will likely depend on the way 'Contract Material' is defined.]
- *Trade marks*: DoCIA may apply to protect the name 'SCAMGuard' as a registered trade mark. Before committing to any branding we might undertake a comprehensive trade mark search. This would include: a search of the Australian Register of Trade Marks in order to identify any prior applications or registrations containing marks that are identical or deceptively similar in relation to the goods and services of interest. It might also include searches of other databases in a preliminary attempt to ascertain whether third parties have common law rights in respect of similar marks. The databases typically searched as part of this process include the Australian company and business names databases, Telstra telephone directory listings, internet domain names (e.g. .org.au, .org, .asn.au, .net.au, .net, .info, .com.au, .com, .biz) and the world wide web generally.
- *Confidential information*: You would need to check the Contract, but it probably also imposes an obligation on NCrypt to safeguard DoCIA's confidential information, which would include the details of the IE9 algorithm.
- *Patents*: Similarly, the algorithm may be the subject of a patent application, depending on our patent attorney's advice.

## Weaknesses

- There is a potential weakness in our copyright ownership. We only have a *licence* (not ownership) in relation to any pre-existing modules (i.e. 'background IP'). So it is important to understand the *scope* of the licence we have.
- In particular, it is not clear from what has been said whether the licence 'for the services of the Commonwealth' applies to the *whole* Commonwealth or just the Commonwealth *as represented by DoCIA*.<sup>6</sup> Because the phrase is reminiscent of section 183, it is likely that it does have the wider meaning. A review of the whole Contract might throw light on the question.
- If we don't have a *voluntary* licence to implement SCAMGuard throughout the Commonwealth, we could consider using the statutory licence in s.183, which would at least enable us to implement the system in the Commonwealth (as originally planned).
- Despite the above points, we could not undertake any *wider* distribution or commercialisation of the SCAMGuard system in a form incorporating the pre-existing modules (as now hoped).
- For these reasons it is important that we identify the pre-existing modules, if any, so that we understand our IP position better. We should check the Contract to see if it provides any mechanism for determining the pre-existing modules, eg an *IP Register*. However do not overlook the obvious: we can *ask* NCrypt.
- Ultimately we need to make an assessment about how critical any pre-existing modules are. We may need to consider negotiating with NCrypt (or third parties) about them. Alternatively (or in case negotiations fail) what are the prospects of re-engineering the modules?

## Opportunities

- We may succeed in achieving wide adoption of the SCAMGuard system, if we can establish our IP position accurately and shore up any weaknesses. This could be good for DoCIA, the Minister and your career.

## Threats

- Delia's casual reference to Google may or may not indicate a problem. We should follow up with NCrypt to satisfy ourselves that they have not copied Google code without a licence, or used

---

<sup>6</sup> See the two references to 'Commonwealth' in the first paragraph of this Scenario.

Google patented technology.<sup>7</sup> We should also check the Contract to see what IP warranties they gave.

- Even if the warranties look watertight we might also engage a patent attorney to advise in general whether our technology infringes any existing patent.
- As mentioned previously, Klaus is currently writing a paper on advanced data mining techniques for publication. We should ensure that he is aware of obligations of confidentiality binding him, and we may wish to vet the paper to ensure that it does not divulge our confidential information or prejudice our prospects of a successful patent application.<sup>8</sup>
- In fact you should probably remind all those connected with the project (including NCrypt) that they should keep the details of the technology secret.

---

<sup>7</sup> It is understood that Google have recently lodged a patent application for their 'PageRank' algorithm, which is therefore now disclosed.

<sup>8</sup> The policy underlying the patent system is that the proprietor obtains a limited monopoly rights in return for disclosure of their invention. If disclosure has already occurred 'the deal is off'.

## 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?

- There is an element of 'working out things as we go along' here. We seem to be allowing NCrypt to treat its obligations far too casually, and to assume a role that is not countenanced under the Contract.<sup>9</sup> There are risks associated with this style (probity; reduced options; less than optimal outcomes). It doesn't inspire confidence and someone (probably you) needs to take charge!

### What might be involved in a 'partnering' arrangement?

- Almost anything really. The reference to a 'partnering' arrangement is legally vague, and (in the absence of further elucidation) not helpful to the tender process. It could entail any of a number of possible commercialisation structures.

### Is Bruce right about the policy?

- Bruce is simplifying the matter. There is no policy that 'requires' that software developers be allowed to retain ownership of the software they develop for Commonwealth agencies, or given rights to commercialise it.
- It would be more accurate to state that each case should be considered on its merits, having regard to factors such as:
  - the corporate mission of DoCIA - was it set up with a commercialisation role?
  - any relevant legislation applicable to DoCIA;
  - the function of the software;
  - the intended user base;
  - which of the parties is best able to maintain and further develop the software?
- A good analysis of possible approaches can be found in the Commonwealth *Guidelines relating to the Management and Commercialisation of Intellectual Property in the field of Information Technology* (the 'IT IP Guidelines') which can be found at: <http://www.dcita.gov.au>.
- You might ask whether DoCIA has an IP Policy in place. If not you might suggest they develop one (you could offer to do it) so that there is clearer guidance about how to balance commercialisation objectives against other DoCIA goals.

---

<sup>9</sup> In particular, it is rather cheeky of them to set up a confidentiality barrier against us!

**Should we commercialise now with NCrypt?**

- As yet, there doesn't appear to be a clear business case for doing so.
- The facts stated suggest there could be probity and 'value-for-money' issues under the Commonwealth Procurement Guidelines ('CPGs') (which bind DoCIA as an FMA Act agency).
- It is not clear whether appointing a Distributor of IP would be classified under the CPGs as a (part) *disposal of property* or engagement of a *service provider*. It probably doesn't matter. Arguably we should adhere to the spirit of the CPGs anyway.
- Thus it might be argued that we should test the market, rather than appoint NCrypt now as Distributor. Pertinent to this: you might inquire whether the tender evaluation process involved a consideration of NCrypt's marketing skills (or merely their development skills).
- If NCrypt do not have proven commercialisation skills, testing the market in a further competitive process might encourage them to enter into a consortium arrangement to complement their skill set.

### 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

- This is a straightforward option (at least it is easy to understand the notion). It has the advantage of preserving all options, and would be easy to change direction at any future time. However, you should conduct a proper Risk Analysis. What are the technical and legal risks associated with commercialisation of the technology? Do we have the skill set in house to undertake commercialisation? Can we apply the resources necessary?

#### 2. Sell option

- This also has the advantage of simplicity. It is probably the best way to avoid commercial risk, which can be shifted to the purchaser.
- You would not take this course, however, to the extent that DoCIA needs to retain control over the standards that lie at the core of the system and/or the future development path of the SCAMGuard system.
- We must ensure that we own what we are purporting to sell (so can give warranties to the purchaser). In relation to the pre-existing modules:
  - we could acquire the rights (or re-write the modules) prior to any RFT, so as to offer the purchaser clear title;
  - alternatively we could offer a partial title on the basis that the purchaser (if someone other than NCrypt) would negotiate with NCrypt (or re-write the modules themselves).
- Would we allow for bids from non-Australian firms (e.g. Google)?

- Do we want to achieve the highest price, or are there other objectives (e.g. promoting wide adoption of the Mapper standard)?

### 3. RFP option

- That might be quite a good option if:
  - we know what technology we want to commercialise and have some idea of the needs of the marketplace;
  - but are undecided what roles DoCIA and the commercial entity should exercise in future development and marketing.
- Nevertheless you may want to impose some constraints on the range of solutions so that you are in a position to compare bids.

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

- Do we mean gross revenue or net revenue? Are there issues in identifying clearly whether any particular revenue relates to the SCAMGuard system, or other technologies that they might exploit, e.g. risk of transfer pricing? If 'net' revenue, what costs and overheads are allowable deductions from gross in arriving at the net figure?
- The Distributorship Agreement should incorporate a Business Plan, and possibly commit NCrypt to the revenue projections they proffered earlier; and/or should provide the option for DoCIA to terminate at will after a reasonable notice period. You may also consider the possibility of defining a revenue stream that is a combination of a one off or periodic licence fee, and royalties based on the volume of business that NCrypt does. That would mean that they will still pay for the distribution rights even if they don't secure sales.

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

- In this case we need to be absolutely clear what constitutes a 'sale' or other 'royaltable event', because our revenue depends on that. It might be wise to attach as a Schedule a required form of End-user Licence. This establishes a known basis of business with end users, so that it is easy to count the transactions that constitute a 'sale'. However it does introduce some inflexibility in the way the Distributor does business.
- Again, the Distributorship Agreement should incorporate a Business Plan, and some options for DoCIA in the event that NCrypt do not meet the revenue projections.

### 6. Other options?

- *JVC option*: we could establish a *joint venture company*, alone or with NCrypt or another commercial party. There are a range of policy constraints applicable here.
- *UJV option*: we could commercialise via an *unincorporated joint venture* with NCrypt or another commercial party. That involves a closer legal relationship than a 'Distributorship' and there are risks that flow from that.

### 7. General comments?

- Note that some of the options involve dealing with NCrypt and some involve a selection process. DoCIA should make an early decision on this threshold question.
- From the information given so far it appears the SCAMGuard involves some 'standard-setting' (especially if it is to be protected by a certification trade mark) and it may be important to retain public ownership and control. Maybe you need to distinguish between the core technology and the less critical 'front end' components or associated applications. You may decide to protect the integrity of the core technology and standards by retaining ownership and/or by registering a certification trade mark. In this respect note the recent report on *Web Seals*<sup>10</sup>. At the same time

---

<sup>10</sup> *Web Seals of Approval - Final Report*, Standing Committee of Officials of Consumer Affairs E-commerce Working Party, January 2005, available at [http://www.consumer.gov.au/html/Web\\_options/](http://www.consumer.gov.au/html/Web_options/). Although not mentioned in the Report, certification trade marks would seem to be the ideal legal vehicle to underpin web seals.

the non-core components could be made available under an open source model which allows a market for commercial firms to provide services to implement, customise and develop. Making the technology free in this way may accelerate its uptake and in the long run may fulfil DoCIA's mission more effectively than if it chases royalties.

#### 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 are involved 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

- In your own interest you should clarify who is your 'employer' during this period. Your employer will own copyright in any materials made by you in the course of your employment. If your employer is equated to the Crown (the Commonwealth) they will additionally own any material made or first published under their 'direction or control' - this is a slightly different test although in these circumstances probably not much turns on that.

- You (and ACAT) need to clarify the working arrangements so that it is clear how the above tests will be applied. To avoid any ambiguity it would be ideal to put in place a written understanding which could encompass: study leave; access to research materials and personnel on which you will draw; your ownership of copyright in the thesis; acknowledging any excerpts of ACAT material; a licence to DoCIA and/or ACAT which permits them to publish a version of the paper (but without them acquiring ownership of the copyright), *etc.* Then everybody should be happy!

#### **What issues arise from our use of the film footage?**

- The proposed use amounts to a *performance in public*.
- If the footage is still in copyright we will need permission from the copyright owner.

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

- The term of copyright in pre-1969 materials may not be the same as for more recent materials.
- Generally, expired copyright does not revive with legislative changes to extend the term.
- The real lesson to be learned is that the duration of old copyright materials is very tricky!

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

- This depends on how we characterise the transaction with the commercial film library. From what has been said it appears quite likely that we have only paid an 'access fee' for obtaining material from their collection. You should look for a copyright statement, or better: an explicit warranty that the film library controlled the relevant IP rights.

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

- The maker of a film has moral rights, including the right of integrity.
- The 'voice over' might be argued to infringe that right, unless we can say it is 'reasonable'; i.e. and ordinary and acceptable practice in the industry.
- Moral rights were only legislated in 2000. In general they are retrospective, although *not* (as it happens) for films.
- Moral rights last as long as the copyright itself.
- What we make of the last two points will therefore depend on whether Chip is right about:
  - how the footage is characterised (in copyright 'subject matter' terms); and
  - whether the footage is still in copyright.

#### **What other issues can you see?**

- Did you get the point that a new copyright arises in the 'voice over' version of the footage?
- Who owns that copyright? Do we need to find out what kind of legal entity ACAT is? ACAT was previously described as a 'joint venture'. However that term can often be used loosely and not much legal confidence can be placed on the way it is described in an Annual Report.

## 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 the clause stating:

**Royalty offset:** *Ownership of any enhancements to Product developed by Licensee<sup>11</sup> shall vest in Licensor<sup>12</sup> 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:

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

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

- Bruce should be kept away from all contracting! He is still making it up as he goes along. The 'royalty offsets' clause is inconsistent with the assumption in the rest of the Agreement that DoCIA will control future development, and the parties' respective roles in that regard need to be resolved.
- In any event it is a very bad idea to hinge IP ownership and entitlement to royalties. Think about the probity and GST issues it presents. Note that there is no defined *mechanism* for making the election to 'fund' development and no indication as to *when* the election must be made. Could you elect one way on one occasion, and differently the next? What happens if the royalties due at any particular time are insufficient to fund development? What about our rights to *audit* the claimed cost of enhancements? Bruce has compounded the problem by agreeing ('in principle' - whatever that might mean) to offset royalties and development cost without quantification on either side of the equation.

### What action should the parties take to clarify IP ownership and royalties due?

- The parties need to clarify whether DoCIA is to 'fund' development of the two new modules. If (despite the concerns outlined above) we are to proceed with that option, you should instruct Chip to prepare documentation to formalise it properly. This will entail proper quantification of: (i) royalties due; and (ii) the cost of development.

<sup>11</sup> NCrypt

<sup>12</sup> DoCIA

- The Agreement should be amended, *either* to remove the 'royalty offsets' clause, *or* to include more effective supporting provisions addressing the issues mentioned above. Failing that, there is a real risk that NCrypt will exploit the provision to our disadvantage. You will find that they are continually improving the SCAMGuard Product, at our cost, to achieve sales. We may be faced with an awkward choice:
  - agree to fund each new batch of enhancements to retain our ownership, at the same time foregoing part or all of the royalties due to us;
  - claim the royalties, but at the cost that our IP ownership of the Product is progressively diluted.

**Do you have the right to terminate the Distributorship Agreement?**

- It is unclear whether the right to terminate at will applies during the 10 year Term, or only during the holding over period.
- On balance, we probably have the right to terminate on 3 months notice during the Term. If it was intended that termination could only happen after 10 years, we might expect to see a comma after the reference to '10 years', and/or the word 'unless' might have been 'until'.

## Denouement

### (in which we get taken to the cleaners)

After it is put into production **SCAMGuard** operates less efficiently than expected, and appreciably slows down internet traffic. Recriminations fly every which way.

Amidst the controversy **Bruce** tosses away his suit and retires to a small place near Nimbin, called Coventry, where he will plot a comeback.

When the email logjam finally clears, months later, two more emails from **Chip** bounce into your Inbox:

Email #4: *You're not going to believe this, but I've thought better of my previous advice! I forgot that s.33(2) only applies to works still in copyright immediately prior to the US FTA amendments. Prior to that, copyright in a photo was covered by s.33(6) which provided for a term lasting 50 years from the year of first distribution. **Except that**, under s.212, if the work was made prior to 1969, s.33(6) does not apply and the term is 50 years from the end of the year when the photo was first taken. I think it's out of copyright. Regards, Chip.*

Email #5: *Oh dear! In my previous advice I relied on ss.33(6) and s.212. I've just noticed that both these provisions have been repealed by the US FTA amendments. I've considered if this means that copyright in a pre-1969 film subsists as a series of photographs under s.33(2) after all? I've decided not. It is likely that the previous sections 33(6) and 212 have taken effect, and the copyright **has** expired. I think I'm getting too old for this . . . [The rest of the email was rather rambling and incoherent.]*

It turns out that **NCrypt Pty Limited** was a front organised by Klaus, and the name is a sort of gothic joke. He is a director of the Company, but that did not come to light because no company search was done. **Meredith** says he used to be a 'nice boy', but turned to the dark side after his ideas for *Inference Engine 5* were cruelly ridiculed and he was passed over for promotion, in favour of Bruce.

It seems that **Klaus** was responsible for the most of the work on SCAMGuard, and had been feeding Delia with the critical code for *Inference Engine 9*, which he was developing in his spare time. This of course raises interesting questions about the ownership of the system.

**Delia's** business is actually listed as dry-cleaning. While Klaus was writing the code, she was busily developing a new process for treating fabrics so that they come out of the wash cleaner and whiter than ever before. She has registered a trademark for the process: '**SCUMGuard**'. You realise that although the name is similar to DoCIA's trademark there is little you can do about it because communications services and dry-cleaning processes are covered in different categories of the Trade Mark Register.

**You** are so impressed with Klaus's subterfuge that you sign him up under an 'Agency Agreement' to tell his story under the working title: '*The scam that ended all scams*'. You include stringent confidentiality obligations, and caution him about continuing his 'blogging' activities. You are careful to include a clause allowing you to assign your rights under the contract. You sit back, content to wait for the day when - you confidently anticipate - you will be approached by your mates from Channel Nine seeking to acquire the rights. You don't expect something on the scale of the latest 'Harry Potter', but it should be a nice little earner.

Indeed the phone call does come, but that's a story for another day.

## Index of IP issues dealt with in Case Study

IP concept / issue	Where and how it arises
accountability for public expenditure	An implicit issue in the choices about when, how and with whom we will commercialise SCAMGuard - see Scenario 2 and Scenario 3.
'acts comprised in the copyright'	The things a copyright owner has an exclusive right to do. For example, the 'public performance' right mentioned in Scenario 4.
auditing	A Distributorship agreement should provide the Licensor with rights to audit royalties, and possibly other aspects of the Distributorship - see Recital 5.
background material	<p>Material brought to an agreement or relationship by one of the parties.</p> <p>In an agreement the service provider often retains IP in the background material, and the customer receives a licence (only) in relation to any background material included in the deliverables.</p> <p>In fact that is the case in Scenario 1, from which it appears there is some background IP that DoCIA does not own. By Scenario 3 we have learned this is not the major problem we feared.</p>
Business Plan	<p>Often a pre-cursor to, or a component of a Distributorship agreement. Needs to be kept up to date. May incorporate revenue and royalty targets.</p> <p>See Scenario 2 and Scenario 3.</p>
certification trade mark <i>versus</i> a conventional trade mark	<p>In Scenario 1 we consider the possibility of protecting 'SCAMGuard' as a (conventional) trade mark.</p> <p>In Scenario 3 we identify the possibility of registering it as a certification trade mark, which would be used to signify ISPs <i>etc</i> who have installed the 'Mapper' component on which the system depends.</p>
character merchandising	<p>The marketing of personalities through endorsements, etc. Not a discrete area of law, but rather based on an amalgam of trade practices law, trade marks, contract, <i>etc</i>.</p> <p>You are a natural at it - see <i>Dramatis Personae</i> and <i>Denouement</i>.</p>
cheek	What NCrypt display in talking to customers without authorisation, and then purporting to withhold the details - see Scenario 2.
commercialisation	<p>For purposes of this Case Study this can be taken to include commercialisation by DoCIA itself, or appointment of (i.e. 'licensing') a Distributor to do it for us.</p> <p>A range of 'commercialisation' options are examined in Scenario 3.</p>
Commonwealth	In software licences to FMA Act agencies, this term can be ambiguous - see Scenario 1.
CPGs	<p>Commonwealth Procurement Guidelines.</p> <p>Scenario 2 raises a question about how a Distributorship should be analysed for purposes of the CPGs.</p>

confidential information	<p>An important means of protecting the core SCAMGuard technology, in particular the IE9 algorithm - see Scenario 1.</p> <p>NCrypt have little respect for their obligations in this regard - see Scenario 2.</p>
conflict of interest	<p>Often relates to misuse of confidential information.</p> <p>Klaus flouts this principle more spectacularly than anyone - see <i>Denouement</i>.</p>
Contract Material	<p>Common term used to describe the IP subject matter created as part of carrying out a contract, i.e. foreground material.</p> <p>In Scenario 1 we consider what parts of the SCAMGuard system are 'Contract Material', and what parts of that we own.</p>
Distributorship	<p>A form of licence agreement, under which the licensee (Distributor) is appointed to commercialise IP material, in return for payment of royalties.</p> <p>A Distributor is usually appointed for a substantial Term.</p> <p>NCrypt first raise the possibility in Scenario 2, and Bruce supports them in Scenario 3.</p> <p>By Scenario 5 they have been appointed. However, the Distributorship arrangements are presenting DoCIA with severe problems in quantifying royalties and determining ownership of IP in enhancements to the system.</p>
employment (relationship)	<p>The importance of it is that copyright in anything created by an employee in the course of that employment is owned by the employer.</p> <p>As we see in Scenario 4, in cases of 'secondment' it may be wise to clarify the ownership question, rather than leave it to general principles. The same can be said in cases of sabbatical and study leave, and situations where an employee makes use of material or resources accessed from their workplace.</p> <p>Did you see the twist in the <i>Denouement</i>?</p>
(cinematograph) film	A category of copyright subject matter. Crops up in Scenario 4.
foreground material	<p>In agreements often called 'Contract Material'.</p> <p>In Scenario 1 we find that DoCIA owns IP in any foreground material created by NSync under the Contract.</p>
infringement	In the case of copyright, usually arises when someone performs an 'act comprised in the copyright' without the permission (direct or indirect) of the copyright owner.
IP Policy	<p>What we could really use to guide us in making choices about DoCIA's commercialisation options.</p> <p>In Scenario 2 we mention the IT IP Guidelines which apply on a 'whole-of-Commonwealth' basis. Policy issues are also involved in Scenario 3 (e.g. whether we seek to promote wide adoption of SCAMGuard, or to maximise our revenue).</p>
IP Regime	A legal form of protection for creative subject matter.

	Copyright, trade marks, confidential information and patents are examples that appear in this Case Study - see Scenario 1.
IP Register	Would help us to identify any 'pre-existing modules' so that we are fully aware of gaps in our IP ownership - see Scenario 1. Might also be useful in Scenario 5 in keeping track of modules that are 'funded' by DoCIA.
joint venture	One of the 'commercialisation' options considered in Scenario 3.  In Scenario 4 we learn the term is often used loosely.
licence	Authorisation by or on behalf of the owner of the relevant IP rights for a third party to do some act in relation to the protected subject matter that the IP owner has the exclusive right to do.  For example, in Scenario 4 we consider the need to get permission from the copyright owner for public performance of their newsreel footage. It is not clear whether the commercial film library has granted a licence or not.  One kind of licence is a 'Distributorship'.
moral rights	In Scenario 4 we consider whether the manipulation of old newsreel footage by adding 'voice over' could infringe the moral rights of the maker, or whether the 'reasonableness' defence might apply. We also consider how long moral rights last.
open source	The merits of making certain components of SCAMGuard available under an 'open source' licence are briefly mentioned in Scenario 3.
partnering	A vague term which could cover a range of 'commercialisation options where a commercial entity is involved.
patent	Scenario 1 raises the possibility of protecting certain components of 'SCAMGuard' under patents law.
probity issues	Probity issues arise briefly in Scenario 2.  See also entries for 'confidential information' and 'conflict of interest'.
RFP	Request for Proposal. See Scenario 3.
royalties	Periodic payments under a Distributorship, based on the volume of commercial activity.  In Scenario 3 we consider the merits of different royalty structuring arrangements.  In Scenario 5 we see how royalty arrangements can get into a muddle.
statutory licence	A licence given by statute (as opposed to an ordinary (voluntary) licence.  An example relevant to this Case Study is s.183 of the Copyright Act, which allows the Commonwealth to use third party copyright materials 'for the services of the Commonwealth', subject to certain requirements. This is an option for DoCIA in relation to the pre-existing modules - see Scenario 1.
subject matter	That which is capable of protection under an IP Regime.  In Scenario 1, we attempt to identify SCAMGuard IP subject matters

	involved in the SCAMGuard system, and the applicable IP Regimes.
tendering	In Scenario 2 there are shifting assumptions between the tender and contract phases, which create probity and 'value for money' issues.
term (of copyright)	In Scenario 4, we learn that it can be complex working out whether the copyright has expired.  In the Denouement we learn that it can be <i>very</i> complex.
Term (of a licence)	The 'Term' is often a key parameter of a licence (including especially an exclusive Distributorship).  The Distributorship arranged with NSync has a Term of 10 years - see Scenario 5.
termination (of a licence)	Bringing it to an end before its ordinary Term has expired.  In Scenario 5 we consider a termination clause containing classic ambiguity.
trade mark	Scenario 1 deals with the possibility of protecting 'SCAMGuard' as a trade mark, and outlines searches we might undertake first.  Trade marks are registered in relation goods or services in a particular <i>category</i> of the Trade Marks Register - see <i>Denouement</i> .  See also above re 'certification trade mark'.
US FTA	United States Free Trade Agreement.  Amendments flowing from the US FTA include extensions to the term of copyright - see Scenario 4 and the Denouement.