Title	Quantification of digital forensic hypotheses using probability theory
Author(s)	Overill, RE; Silomon, JAM; Chow, KP; Tse, HKS
Citation	The 8th International Workshop on Systematic Approaches to Digital Forensics Engineering (SADFE 2013), Hong Kong, 21-22 November 2013. In Conference Proceedings, 2013, p. 1-5
Issued Date	2013
URL	http://hdl.handle.net/10722/203655
Rights	International Workshop on Systematic Approaches to Digital Forensics Engineering (SADFE). Copyright © IEEE.

Quantification of Digital Forensic Hypotheses Using Probability Theory

Richard E Overill and Jantje A M Silomon
Department of Informatics
King's College London
Strand, London WC2R 2LS, UK
richard.overill@kcl.ac.uk | jantje.silomon@gmail.com

Kam-Pui Chow and Hayson Tse
Department of Computer Science
University of Hong Kong
Pokfulam Road, Hong Kong
chow@cs.hku.hk | hayson.tse@gmail.com

***Abstract*— The issue of downloading illegal material from a website onto a personal digital device is considered from the perspective of conventional (Pascalian) probability theory. We present quantitative results for a simple model system by which we analyse and counter the putative defence case that the forensically recovered illegal material was downloaded accidentally by the defendant. The model is applied to two actual prosecutions involving possession of child pornography.**

Keywords*— *Probability theory; digital forensics; quantification of plausibility; digital forensic hypotheses; possession of child pornography.

I. INTRODUCTION AND BACKGROUND

Conventional forensic practitioners have an admirable tradition of employing statistical techniques and probability theory to interpret their findings quantitatively for prosecution authorities and courts of law. For example, the probability that two identical DNA samples do not arise from the same individual has been quantified as approximately one in a billion, whereas the probability of two matching fingerprints belonging to two different individuals is rated at one in a million.

Digital forensic practitioners, by contrast, have been slow to follow suit, generally preferring to make qualitative statements about the significance of their evidence. In an effort to introduce a degree of quantitative rigour into the field of digital forensics the application of Bayesian networks [1–6] and aspects of complexity theory [7–10] has recently been explored as a means of quantifying the plausibility of digital forensic hypotheses. The present paper aims to extend this approach by utilising conventional probability theory to analyse and interpret the significance of recovered digital forensic evidence.

Prosecutions for the possession of illegally downloaded material have caused serious problems for digital forensic examiners and prosecution authorities for well over a decade. Previous studies [7–10] have analysed the plausibility of the Trojan Horse Defence (THD) [11–15], which has frequently been successfully employed against prosecutions for the possession of child pornography (CP) images [10, 16–17].

In this paper we address another commonly offered defence against the possession of CP images, when only a small proportion of the recovered downloaded material is illegal. A typical real-world example is the recovery of a small number of CP images amongst a much larger number of adult pornography (AP) or other images. In such a situation, the defence might claim that the defendant only intended to download non-CP images, but because the website also happened to contain some CP images intermixed, a few of these were accidentally or unintentionally downloaded along with the intended non-CP images.

What credence can be given to such a claim, ceteris paribus (everything else being equal)? In particular, what proportion of CP images needs to be present in the download in order for the prosecution to refute the defence's claim beyond a reasonable doubt? In the present paper we address these questions by means of conventional probability theory applied to a number of distinct scenarios based on two actual criminal cases. In order to carry through the analysis it has been necessary to make a number of simplifying assumptions regarding the downloading context and these have been itemised below.

In the next section we present our analytical models and set out the principal assumptions upon which they are based. Our results for two fully-documented criminal cases are to be found in the subsequent sections, where they are discussed and interpreted in the context of the relevant legal framework. The final section contains our summary and conclusions, together with a generalisation of the domain of applicability of our analytical models.

II. PROBABILITY THEORETIC MODELS

Let the number of distinct downloaded CP images be n_c, and the number of distinct downloaded AP or other images be n_a. Thus the total number of distinct downloaded images recovered is $n_d = n_c + n_a$.

Since the precise contents of the overseas websites from which each of the downloads was made cannot usually be investigated by the local law enforcement officers, it is necessary to make the assumption that the proportion of CP images in the download reflects the proportion of CP images in the website as a whole (i.e. that the download is a representative sample of the website). Let the (unknown) total number of images available for download from the website be N, then the estimated number of CP images on the website is

Sponsored by IEEE Louisville Chapter.
978-1-4799-4061-5/13/$31.00 ©2013 IEEE

$N_c = N \times (n_c / n_d)$ and the estimated number of non-CP images is $N_a = \mathrm{N} \times (n_a / n_d)$ where $N = N_c + N_a$.

We wish to determine expressions for the probability P_k that precisely k ($0 \leqslant k \leqslant \min[N_c, n_d]$) distinct CP images are present amongst the n_d distinct downloaded images. For this purpose we assume that the website is organised in such a way that any CP images are located randomly amongst the non-CP images, rather than in a special section, so that the website owner could plausibly claim that the CP images were uploaded inadvertently. We consequently assume that the defendant encounters the CP images randomly while browsing the website contents and selected the image thumbnails for downloading as an integral part of the browsing operation.

Within the context outlined above, three distinct scenarios can be distinguished. We have termed these scenarios: infinite, finite and greedy, respectively. In the infinite scenario, the number of distinct images available for download from the website is so large that it is effectively infinite and therefore the probability of selecting either a CP image or an AP image does not change as the download proceeds. In the finite scenario, the number of distinct images available for download from the website is definite and so the probabilities of selecting a distinct CP or AP image vary with the progress of the download. The greedy scenario is a special case of non-random behaviour in which the defendant downloads the complete contents of the website; in this case $n_c = N_c$; $n_a = N_a$; $n_d = N$.

A. *Infinite scenario*

Since the probabilities of selecting a CP image and a non-CP image are both fixed at $p_c = (N_c / N)$ and $p_a = (N_a / N)$ respectively, where $p_c + p_a = 1$, the binomial theorem [18] can be applied directly:

$$P_k = \binom{n_d}{k} p_c^k \, p_a^{n_d - k} \tag{1}$$

Here $\binom{n_d}{k}$ is the number of different ways of selecting k objects from n_d distinct objects.

B. *Finite scenario*

The probabilities of selecting a CP image and a non-CP image both vary as the images are being selected, on the assumption that no image is downloaded more than once. This is equivalent to the well-known scenario of selecting k black balls and $(n_d - k)$ white balls randomly from a bag initially containing N_c black balls and N_a white balls respectively:

$$P_k = \binom{n_d}{k} \prod_{i=0}^{k-1} \frac{N_c - i}{N - i} \prod_{j=0}^{n_d - k + 1} \frac{N_a - j}{N - k - j} = \binom{N_c}{k} \binom{N_a}{n_d - k} \Big/ \binom{N}{n_d} \tag{2}$$

Here the first and second products address the probabilities of selecting black and white balls respectively. Note that the right-hand expression, although elegant, is not suitable for practical computations involving large integer values such as will be encountered later, where the left-hand expression is implemented instead.

C. *Greedy scenario*

Since the defendant downloads the entire contents of the website it is certain that precisely $n_c = N_c$ CP images and $n_a = N_a$ AP images are downloaded. Hence the probability distribution is singular:

$$P_k = \delta_{k,n_c} \tag{3}$$

Here $\delta_{ij} = 1$ if $i = j$ and 0 if $i \neq j$ is Kronecker's delta [18].

III. Two Case Studies

Two actual criminal cases from the District Court of the Hong Kong Special Administrative Region (HK SAR) involving the possession of CP images are now studied in more detail.

Case 1: In District Court Criminal Case No. 968/2010, the defendant had over 30,000 image files which he had downloaded on various occasions. Amongst them, there were 63 still images and 185 video clips, all 248 of which image files were of CP. The others were indecent and obscene materials, plus cartoons and comic story books.

Case 2: In DCCC No. 32/2013, the defendant had 714,430 image files (including still images and video clips) which he had downloaded on various occasions. Amongst them, there were 84 video clips which were of CP. The others were indecent and obscene materials.

In both cases, the image files were downloaded over a substantial period of time, involving a number of separate downloading sessions, making use of more than one website. All of the recovered image files had been opened and viewed by the defendants, on their own admission, so no metadata evidence was collected by law enforcement investigators to verify this independently.

The legal documentation regarding prosecution for possession of CP in HK SAR are available for reference [19–22], but for the purposes of this discussion they may be summarised as follows. Section 3(3) makes it an offence for any person to have in his possession any CP materials. The elements of the offence of possession of CP are: (i) possession (i.e., having custody or control) of the image files; and (ii) knowing the nature of the image files' contents (i.e., being CP). Thus, a bare confession that: "I downloaded them" and "I opened them to view" is sufficient. In the absence of such a confession, the prosecution needs to demonstrate both (i) and (ii) beyond a reasonable doubt. In particular, (ii) requires the prosecution to show that the defendants knew that they possessed something (*mens rea* or 'guilty mind') and that the something they possessed was indeed CP (i.e., that it contained a pornographic depiction, and that the subject of that depiction was a child under the age of 16 years). The defendants could in principle have pleaded not guilty and fought the prosecution case, claiming that they did not view any of the downloaded images or that they viewed them only as thumbnails and hence did not see them clearly enough to be able to make an informed judgment regarding the ages of the depicted individuals.

IV. Results and Discussion

The quantitative results for both the infinite and finite scenarios of both actual cases are presented in Table 1. For the finite case, the representative value for N has been (somewhat arbitrarily) chosen as the smallest power of 10 greater than n_d. Thus, for case 1, n_d = 30,000 and $N = 10^5$, while for case 2, n_d = 714,430 and $N = 10^6$. Values of P_k are set out for k = 1, 10, 20, n_c /4, n_c /2 and for the maximum of the distribution at $k = n_c$, where k represents the number of downloaded CP images. In Figures 1 – 4 the four probability distributions are shown graphically over the range $0 \leqslant k \leqslant \min[N_c, n_d]$. Note that in Figure 3 the probability distribution is truncated at k=118 which is the value of N_c in this case. It should be mentioned here that these computations require the use of extended range programming techniques since intermediate values with magnitudes in the range $[10^{-1000}, 10^{1000}]$ are created, which lie well beyond the range available from the IEEE-754 64-bit floating-point representation of $[10^{-322}, 10^{322}]$.

Inspection of Table 1 and Figures 1–4 reveals a number of interesting features. Although the probability distributions are quite strongly peaked and not greatly skewed, their maxima at $k = n_c$ all lie between 2.5% and 8%. That is, there is at the very most a chance of 2.5%–3.0% in case 1 and 4.0%–8.0% in case 2 that the CP image files were downloaded by means of inadvertent, random behaviour on the part of the defendant. The difference between the infinite and the finite scenarios in each case is directly related to the numerical ratio between n_d and N; in case 1, N:n_d = 3.333, whereas in case 2, N:n_d = 1.400. As a consequence, in case 1 the finite scenario reproduces the infinite scenario much more closely than in case 2 where N is only slightly greater than n_d. In both cases, the finite scenario yields a higher maximum probability than the infinite scenario due to the restriction of the number of images on the website to N in the finite scenario. The variances of the binomial distributions for cases 1 and 2 (infinite scenarios) are both very close to their respective means at 245.95 and 83.00, while their skewnesses are 0.0627 and 0.1091 respectively. *Ca.* 95% of the probability density is located within the ranges k= [217, 279] or ±12.6% for case 1 and k= [66, 102] or ±21.7% for case 2. The probability of accidentally or unintentionally downloading k CP images is exceedingly small, although always non-zero, towards the tails of the distribution (see the topmost lines of Table 1). However, even close to the mean the probability lies well below 10% in both scenarios of the two actual cases studied here.

It will be noted that the models presented here make a number of simplifying assumptions about the downloading behaviour of the defendant, namely: a single session, a single website, a single user and a single computer. In fact it took the defendant in case 2 around two years to download the 714,430 image files from several websites. However, it appears unlikely that these assumptions would invalidate our model since a defendant's behaviour would be expected to remain fairly consistent between successive sessions and websites.

Since no corroborating metadata was recovered by the law enforcement officials, it is not known for certain whether either of the defendants had actually opened and viewed the CP image files; their admissions of guilt were accepted in lieu of locating such evidence. Had the defendants elected to plead not guilty, not only would the metadata associated with their CP image files have had to be located and recovered, but the accuracy of the age discrimination between the CP and AP images might also have been challenged.

Furthermore, under some circumstances it might be possible for the defence to argue that the number of downloaded CP images files was not sufficiently statistically significant to be considered a representative sample of the website contents as a whole. In particular, if the defendants were to claim that they were searching for a particular type of non-CP image then their searching and selecting strategy might not conform to the random browsing and downloading behaviour envisaged in the present model.

One final comment is in order: if a website that the defendant browsed was promoted or advertised as containing only non-CP material, the defendant might claim that the downloaded CP images were present as the result of a content management error on the part of the website's owner. This could lead to contention over the responsibility for the presence and distribution of the CP material – a case of *caveat emptor* (let the customer beware) or *in dubio pro reo* (when in doubt find for the accused)?

V. Summary and Conclusions

In this paper we have shown how conventional probability theory can be used to provide answers to questions that digital forensic examiners and prosecution authorities are likely to pose with regard to the presence of a small proportion of CP image files amongst a large number of downloaded non-CP image files. By making some simplifying but not unreasonable assumptions about the image selection and downloading process we have shown that in the very worst case (from the prosecution's perspective) the probability of this occurring unintentionally in the two actual cases studied here is 2.5–3.0% and 4.0–8.0% respectively. The principal conclusion to be drawn from our results may be summarised as follows: the probability of randomly downloading a small number of CP files amongst a large number of non-CP files is in general exceedingly small and, even at its maximum, lies well below 10% in both scenarios of the two actual cases studied here. Results such as these can be used to provide a quantitative input into the decision-making processes of law enforcement and prosecution authority officials. While we are aware of complementary approaches using subjective probability assessment, for example [23], our aim here is to be as rigorously quantitative as possible.

A related issue for law enforcement investigators is that a full confession is more easily elicited from a suspect when they are confronted with a full account of their actions as reconstructed from the recovered evidence. Thus, it may be considered that the police were fortunate to secure confessions in the two actual cases studied here, without first having recovered detailed meta-data evidence to place before the suspects. It should be regarded as standard professional due diligence to do so, rather than to rely on eliciting a confession. It would also be interesting to compare the two Hong Kong cases studied here with those from other jurisdictions.

The approach described here is by no means restricted to illegal downloads of CP material. It is capable of being applied to a much broader class of problems, most notably in the commercial and business world. For example, an employee is accused of stealing company confidential information and a number of such files are found in his PC desktop. Does this constitute sufficient grounds for civil litigation? How likely is it that the files were downloaded and then forgotten to be removed? As a second example, an employee is accused of attacking the company network but only a few incidents of short duration were actually detected. Does this constitute sufficient grounds for a criminal prosecution?

This raises a more general question: in the digital or cyber domain, there are many human initiated events that are anomalous and potentially illegal; how many such events should be considered sufficient to warrant further action in terms of either a civil or a criminal prosecution? We consider this to be a question that merits further study in the future.

TABLE I. SELECTED VALUES OF THE PROBABILITY OF RANDOMLY DOWNLOADING K CP IMAGE FILES IN CASES 1 AND 2 ACCORDING TO THE FINITE AND THE INFINITE SCENARIOS.

	Case 1 (n_d=30,000, n_c=248)		**Case 2 (n_d=714,430, n_c=84)**	
	Finite ***($N=10^5$)***	***Infinite***	***Finite*** ***($N=10^6$)***	***Infinite***
k	P_k	P_k	P_k	P_k
1	6×10^{-127}	2×10^{-106}	6×10^{-62}	3×10^{-35}
10	2×10^{-110}	2×10^{-91}	5×10^{-47}	2×10^{-24}
20	7×10^{-97}	3×10^{-79}	1×10^{-34}	4×10^{-17}
$n_c/4$	1×10^{-57}	1×10^{-45}	1×10^{-33}	2×10^{-16}
$n_c/2$	3×10^{-24}	8×10^{-19}	6×10^{-16}	2×10^{-7}
n_c	0.0304	0.0254	0.0807	0.0435

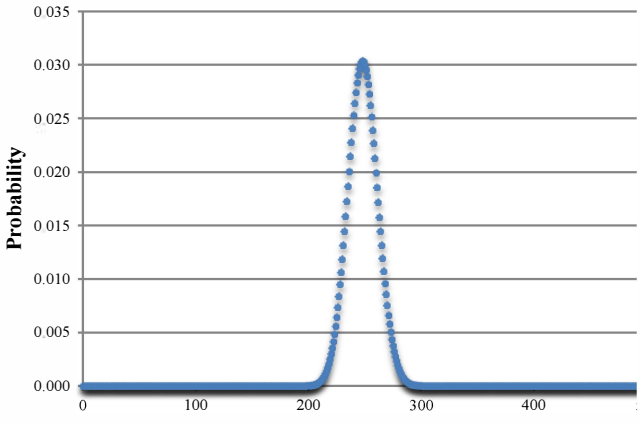

Fig. 1. Probability distribution function for case 1, finite scenario

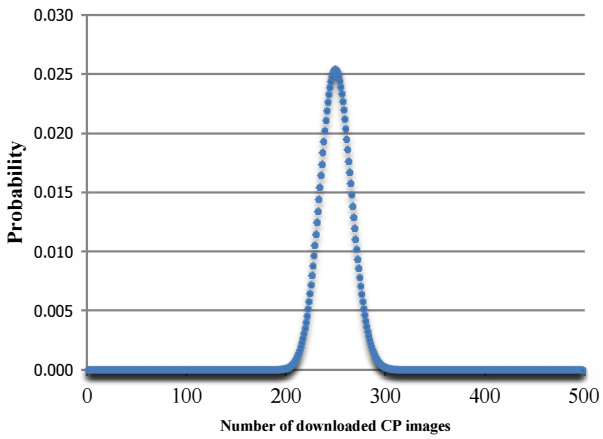

Fig. 2. Probability distribution function for case 1, infinite scenario

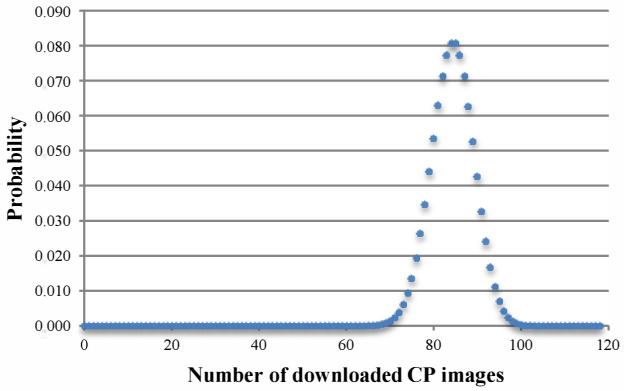

Fig. 3. Probability distribution function for case 2, finite scenario

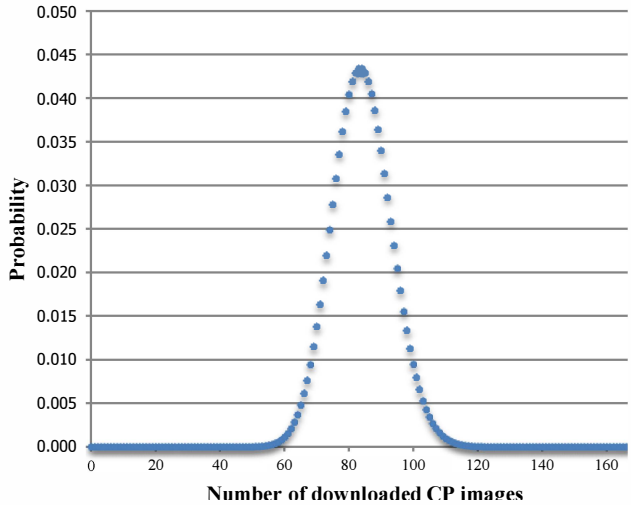

Fig. 4. Probability distribution function for case 2, infinite scenario

REFERENCES

[1] Kwan, M, Chow, K, Law, F and Lai, P, Reasoning about evidence using Bayesian networks, Advances in Digital Forensics IV (2008) Springer, pp.275—289.

[2] Kwan Y K, Overill R E, Chow K P, Silomon J A M, Tse H, Law Y W and Lai K Y, Evaluation of Evidence in Internet Auction Fraud Investigations, Proc.6th Annual IFIP WG 11.9 International Conference on Digital Forensics, Hong Kong, 3-6 January 2010, Advances in Digital Forensics VI, Ch.7, pp.95–106, Springer (2010)

[3] Overill R E, Silomon J A M, Kwan Y K, Chow K P, Law Y W and Lai K Y, Sensitivity Analysis of a Bayesian Network for Reasoning about Digital Forensic Evidence, 4th International Workshop on Forensics for Future Generation Communication Environments (F2GC-2010), in Proc. HumanCom-2010: 3rd International Conference on Human-Centric Computing, Cebu, Philippines, 11-13 August 2010, IEEE Press, pp.228–232.

[4] Kwan M, Overill R, Chow K-P, Tse H, Law F and Lai P, Sensitivity Analysis of Digital Forensic Reasoning in Bayesian Network Models, Advances in Digital Forensics VII, pp.213–244, Springer (2011), Proc. 7th Annual IFIP WG 11.9 International Conference on Digital Forensics, Orlando, Florida, USA, 30 January - 2 February 2011.

[5] Overill, R E and Silomon, J A M, Six Simple Schemata for Approximating Bayesian Belief Networks, in Cyberforensics: Issues and Perspectives, Proc 1st International Conference on Cybercrime, Security and Digital Forensics (ed. GRS Weir), Glasgow, UK, 27-28 June 2011, pp.65–72.

[6] Overill, R E, Zhang, P and Chow, K-P, Multi-parameter Sensitivity Analysis of a Bayesian Network from a Digital Forensic Investigation, Proc. 2012 ADFSL Conference on Digital Forensics, Security and Law, Richmond, Virginia, USA, 30-31 May 2012, pp.149-160.

[7] Overill R E, Silomon J A M and Chow K P, A Complexity Based Model for Quantifying Forensic Evidential Probabilities, Proc. 3rd International Workshop on Digital Forensics (WSDF 2010), Krakow, Poland, 15-18 February 2010, pp.671–676.

[8] Overill, R E and Silomon, J A M, A Complexity Based Forensic Analysis of the Trojan Horse Defence, Proc. 4th International Workshop on Digital Forensics (WSDF 2011), Vienna, Austria, 22-26 August 2011, pp.764-768.

[9] Overill, R E and Silomon, J A M, Uncertainty Bounds for Digital Forensic Evidence and Hypotheses, Proc. 5th International Workshop on Digital Forensics (WSDF 2012), Prague, Czech Republic, 20-24 August 2012, pp.590–595.

[10] Overill, R E , Silomon, J A M, Chow, K-P and Law, Y W, Quantitative Plausibility of the Trojan Horse Defence against Possession of Child Pornography, Proc. 1st International Conference on Digital Forensics and Investigation (ICDFI 2012), Beijing, China, 21-23 September 2012, available online at http://secmeeting.ihep.ac.cn/Program.htm

[11] George, E, UK Computer Misuse Act – the Trojan Virus Defence, Digital Investigation, 1 (2) (2004) 89.

[12] Haagman, D and Ghavalas, B, Trojan Defence: A Forensic View, Digital Investigation, 2 (1) (2005) 23–30.

[13] Ghavalas, B and Philips, A, Trojan Defence: A Forensic View, part II, Digital Investigation, 2 (2) (2005) 133–136.

[14] Mason, S, Trusted Computing and Forensic Investigations, Digital Investigation, 2 (3) (2005) 189–192.

[15] Brenner, S W, Carrier, B and Henninger, J, The Trojan Horse Defence in Cybercrime Cases, Santa Clara Computer & High Tech. Law J., 21 (1) (2004) 9–61.

[16] Chow, K P, Law, Y W F, Kwan, Y K M and Lai K Y, The Rules of Time on NTFS File System, Proceedings of the Second International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE '07) IEEE Computer Society Washington, DC (2007) pp. 71–85.

[17] Law Y W F, Chow, K P, Lai, K Y P, Tse K S H and Tse, W H K, Digital Child Pornography: Offender or not Offender, in Technology for Facilitating Humanity and Combating Social Deviations: Interdisciplinary Perspectives (Eds. Martin, V M, Garcia-Ruiz, M A & Edwards, A), Information Science Reference, IGI Global (2011), Ch.1.

[18] Abramowitz M and Stegun I A, A Handbook of Mathematical Functions, Dover Publications (1965) pp.10, 822.

[19] Prevention of Child Pornography Bill, 2 June 2002, available at: <http://www.gld.gov.hk/egazette/pdf/20020602/es3200206022.pdf>

[20] Prevention of Child Pornography Ordinance, 19 December 2003, available at: <http://www.legislation.gov.hk/blis_pdf.nsf/6799165D2FEE3FA94825755E0033E532/CFAA292BD52BAF67482575EF001E9C6B/$FILE/CAP_579_e_b5.pdf>

[21] Hong Kong Legislative Council paper CB(2)58/02-03(01), Prevention of Child Pornography Bill "Knowingly", October 2002, available at: <http://www.legco.gov.hk/yr01-02/english/bc/bc57/papers/bc571017cb2-58-1e.pdf>

[22] Hong Kong Legislative Council paper CB(2)2631/02-03, Report of the Bills Committee on Prevention of Child Pornography Bill, 23 June 2003, available at: <http://www.legco.gov.hk/yr01-02/english/bc/bc57/reports/bc570709cb2-2631-e.pdf>

[23] Keppens, J, Towards Argumentation about Subjective Probabilities, Proceedings of the Fourth International Conference on Computation Models of Argumentation (2012) pp.422–429.