Introduction

I have been invited to respond to the above mentioned paper (the "*Levy/Robinson*" paper) with the intention that my contribution to the discussions regarding it is circulated and discussed at GCHQ and elsewhere in Government and the Civil Service.

In responding I have attempted to keep my contributions brief. However, because illustrations can often explain matters better than words alone, I have chosen to include some drawings in my responses. My use of illustrations within this paper are "*fair dealings*" within the exemptions granted in the Copyright Designs and Patents Act 1988 (as amended) given the intended limited circulation of this paper. All mistakes and errors in this paper are my own.

In September 2022, in my personal capacity, I filed a seven page paper at Ofcom under their Call for Evidence on the **Online Safety Bill**. This was titled "*Some measures to improve the effectiveness, enforceability and universality of the UK Online Safety Bill*". This response to the Levy/Robinson paper is complementary to my seven page Ofcom paper.

The Home Affairs Select Committee - 2018

The 70 page Levy/Robinson paper is replete with ways in which metadata standards can be used to improve child safety without descending into censorship. Their statements, in depth, echo what **Chief Constable Simon Bailey** initially said in 2018. At this time Simon Bailey was lead for Child Protection at the National Police Chief Council (**NPCC**). When asked by the Home Affairs Select Committee what were the '*key asks*' of industry from Law Enforcement he responded:

- Pre-screening/Pre-filtering of material uploaded and downloaded;
- Industry Platforms to have appropriate safeguards and be '*kite*' marked as a safe environment;
- Industry to ring-fence a proportion of their R&D budget to develop and design safeguards into all of their products.

This was the Joint Position between the NPCC and the National Crime Agency (**NCA**). Five years on we are still waiting - this is therefore something which needs to be delivered by the **Online Safety Bill**. My strong recommendation is that these three "*key asks*" - all of which are related to metadata labelling and are supported in the Levy/Robinson paper - are mandated. Furthermore, the light touch "*comfort letter*" regulatory approach suggested at the end of my Ofcom paper in respect of "*ZachsLaw*" is ideally suited to active R&D child safety interventions.

Metadata labelling if done in accordance with a global standard can enable the quick and effective removal of potentially harmful content without censorship through the use of lightweight filters. This would greatly reduce the areas which the security services and the NCA need to actively police and review content[1] . It is also the only way in which there could be an effective UK "*CyberTipline*" service which adhered to Ofcom transparency and openness requirements given the numbers involved[2].

Furthermore the need for "*Outcome21*" peer to peer protections, so that children are not criminalised for just being curious and social amongst their peers, can only be implemented in accordance with global standards.[3] Client side protections require economies of scale which can only be deployed in accordance with a standard that does not create commercial barriers to new entrants or protected silos for the incumbents. Failure to implement these measures could also result in some long tail risks as youthful behaviour resurfaces from web archives in a child's adult life - this has already been identified as a long term security risk by unfriendly foreign state actors building dossiers for blackmail at a future time.

At page 37 under **5.1.5 Safeguarding content** the Levy/Robinson paper says:

> Services could, at the request of a child or their parent/guardian or by default for all children, add safeguarding functionality to a child's account, giving some other party access to content (and/or metadata), facilitating supervised use of the service. We note that this may drive some children away from services that implement these sorts of techniques.

[1] Referred to at Page 3 of the Levy/Robinson paper
[2] See page 13 of the Levy/Robinson paper for the citation of the numbers of offenders involved which are very large
[3] See page 15 of the Levy/Robinson paper for the citation of the numbers of children at risk of being criminalised

The detailed arguments set out in the Levy/Robinson paper on this topic strongly suggest that the right solution is to mandate "*safeguarding content*" on **all** services which are used by children so that children are not able to access services which do not have a safeguarding functionality. In my view the best way to do this is via "*age gating*" associated not with the child's actual age (which can give rise to tracking, blackmail and abuse) but by reference to the child's school age which is stored as a cryptographically secure token on digital devices. This point was addressed in my seven page Ofcom paper.

However, the Government should be aware of the strong commercial forces which are likely to be deployed against this minimal interventionist approach - particularly from the new entrants in the advertising industry who have historically had a very cavalier attitude towards child protection on the internet and regulation in general. At page 42, the Levy/Robinson paper says:

> Finally, we consider regulatory capture. This is the phenomenon where a regulator acts in the interests of a small number of those it seeks to regulate at the expense of a much larger population. Many of the child protection charities that manage these databases are at least partly funded by the big tech companies whose services are the subject of this discussion and so it is reasonable to ask how we can be certain that the service owners are not manipulating the curation of the database. …"

I am less sure than the Levy/Robinson paper's authors that this manipulation is unlikely to take place. When the UK was part of the EU, Ofcom was unable to protect children in the UK from harms arising from the then EU Audio-Visual Media Services (AVMS) directive which had been the subject of serious lobbying by the new entrants to the internet advertising industry in Brussels[4]. Prior to the UK's period of EU membership traditional television advertising in the UK had been highly regulated to the benefit of parents (and children) who had always been able to trust that a child watching a British commercial television programme would not come to harm from watching the adverts or the programme itself. Global standards are a means by which the UK could enable these protections in an effective manner to the benefit of British society, its broadcasters and advertising industries.

Client side image scanning and safeguarding prompts have similarities to the historic Ofcom pre-approval requirements in respect of television advertising where nothing is transmitted unless it is "*legal, decent, honest and truthful*". A light touch regulatory system, paid for by the industry to be regulated, which requires pre-filtering and pre-labelling of content and

[4] This fact is supported by my personal correspondence with the Director General of Ofcom in 2013/14 where I was notified that "Any changes to enforce the watershed more broadly, to include regulated on-demand content delivered to television sets, would require more than a simple Ofcom rule change. It would instead require a significant change to legislation at either a UK or European level; and any such change to legislation will be a matter for the Government to consider, rather than Ofcom."

advertisements to facilitate their automated filtering without censorship, is socially and politically essential for a free society.

The remaining parts of my response to the Levy/Robinson paper now address an issue which I have previously spoken of to GCHQ when it came to my attention in 2020. It illustrates the central role to be played by metadata labelling in combating fraud and money laundering in the advertising industry.

How the Advertising Industry is funding "Click-Fraud" and Terrorism

An accounting failure

The current UK method of tracking addressable advertising on regulated British television is in breach of fundamental accounting principles. I believe that this situation has arisen not by intention but by accident. However it needs urgent action by the Government.

Background

The **Companies Act 1985** had a section within it that most people have now forgotten about - **Section 722**[5]. These provisions pre-dated the 1985 Act and were grounded in fundamental accounting principles that date back to bookkeeping *alla veneziana* ("the Venetian method"). This section read as follows:

> **722(1)** Any register, index, minute book or accounting records required by the Companies Acts to be kept by a company may be kept either by making entries in bound books or by recording the matters in question in any other manner.
>
> **722(2)** Where any such register, index, minute book or accounting record is not kept by making entries in a bound book, but by some other means, adequate precautions shall be taken for guarding against falsification and facilitating its discovery.
>
> **722(3)** If default is made in complying with subsection (2), the company and every officer of it who is in default is liable to a fine and, for continued contravention, to a daily default fine.

When British Telecom was privatised, under Section 21 of the British Telecom Act 1981 it had to be exempted from compliance with these basic accounting requirements because the then Strowger Telephone


BILL FOR TE_EPHONE SERVICE

POST OFFICE
BRADFORD
TELEPHONE AREA
Telephone House
11 Broadway
BRADFORD
West Yorkshire
BD1 1BA
Telephone: Bradford 23444
(STD Code 0274)
Telex: 51220 (TELMAN BRADFORD)

1131 BOLTON RD
BRADFORD
W YORKSHIRE
BD2 4SP

VAT REG. NO. 243 1700 02

Telephone Number 81 BNC 6502 BRADFORD 651715 Date of bill Tax Point 26 JAN 76

PAYMENT IS NOW DUE AND SHOULD BE MADE WITHIN 14 DAYS. NOTES ON PAYMENT ARE OVERLEAF

	£.
Rental (and other recurring charges) at quarterly rate of £ 8.25 1 JAN to 31 MAR	8.25
Non-recurring charges (statement enclosed) Dialled units to 13 JAN 193 at 3 p.	5.79
Local calls via operator to hand on 16 JAN	
Trunk calls via operator to hand on 18 NOV	0.42
26 NOV	0.98

Any call charges not to hand when this bill was prepared will be included in your next bill.

[5] https://www.legislation.gov.uk/ukpga/1985/6

Exchanges could not comply with these provisions.

For example, on the right is a sample UK Post Office telephone bill from 1976. This contains an entry for ***"193"*** *dialled units for a period between* ***1st January and 31 March 1976***

Itemised billing for telephone calls was impossible at the time. Only when the British telephone system went digital under System X was it possible to comply with the fundamental *alla veneziana* accounting requirement.

To lay people during the 1990s I explained the meaning of **Section 722** of the Companies Act 1985 as follows:

Section 722 says:

* **You may keep your accounting records by employing a clerk sitting on a high stool writing up the records using a quill pen in a bound ledger.**
* **You may also keep your accounting records using any other system of recording**

HOWEVER:

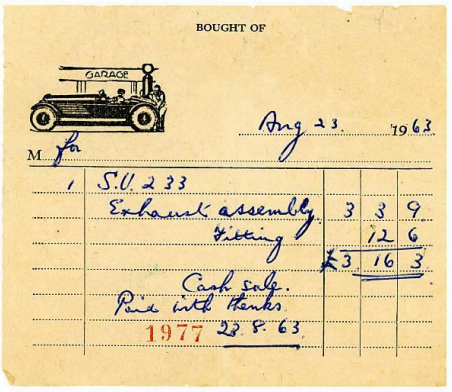
* **If you choose to use ANY other method of recording, other than employing a clerk sitting on a high stool writing up the records using a quill pen in a bound ledger, then you must have equivalent means of ensuring that the accounting records are correct, accurate and cannot be fraudulently altered or amended or forged.**

FAILURE to do so is a CRIME which can lead to:

* **Imprisonment AND**
* **A daily default fine**

Thus if there was a go-ahead Victorian company which decided to use a **loose-leaf ledger** instead of a traditional **bound ledger** (see illustration on the right) there needed to be measures to ensure that it was not possible to substitute pages in the loose-leaf ledger. The standard way in which this was done was through the use of machine printed numbers - a **serial number** on each page of the loose-leaf ledger (not a handwritten number) which provided evidence that showed whether or not a page had been removed or substituted. All entries in the loose-leaf ledger had to be in permanent ink rather than in pencil so that alterations were clear and visible. These accounting requirements were supported by the criminal sanction.

This requirement also applies to receipts and invoices. The unique **serial number** is a key element in invoicing and accounting but its importance appears to have been lost is the rush to "*dematerialised transactions*" on computers and the web. To the right is a sample invoice from 1963 for the sale and fitting of car parts in a garage in a cash transaction - it contains in red a **machine printed number.** The risks of fraud and substitution were well understood in this manual system and consequently security and auditability were coterminous.



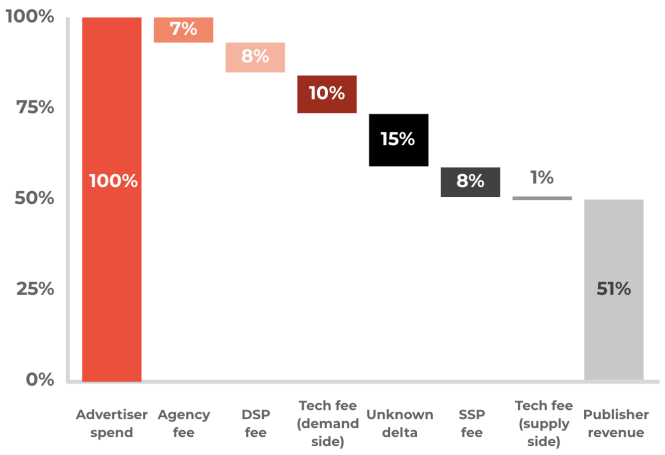
Fundamental Accounting failures arising out of the use of the Clearcast Clock Number in Addressable Advertising

Global Advertising spending is about half a trillion dollars a year - it is the driver behind broadcasting all over the world. As in any major industry, there are core accountancy and compliance requirements.

The first requirement is **Traceability** - when an advertisement is made the Brands, Advertising Agencies, Technology suppliers, broadcast platforms and websites need to establish "*when and where the advert was produced and by whom*." - all the parties in the supply chain must be traceable.

Then you need to be able to **Audit** the transaction - money is paid so taxes are payable, everything needs to be itemizable so that it can be recorded and accounted for by the Brands, Advertising Agencies, Technology suppliers, broadcast platforms etc in accordance with international corporate accounting standards.

Finally in any industry you need to be able to **Prevent Fraud** - when half a trillion dollars a year is at stake organised crime always tries to take a share and you have to design in defence against this - it is not something you can add in later.



In early 2018 the Incorporated Society of British Advertisers (ISBA) undertook a forensic end-to-end study, to try to find out where money went in addressable advertising as it passed through the various intermediaries from advertiser to publisher. Working in partnership with the AOP (Association of Online Publishers) whose members provided the publisher data, and commissioning PwC to connect and audit supply and demand, the ISBA/PwC Programmatic Supply Chain Transparency Study attempted to follow the money flows through the addressable advertising system. Very early on it established that **88%** of advertising impressions could not be fully traced through a spaghetti map of programmatic suppliers and operatives. Only **51%** of advertiser programmatic budgets reached publishers; **15%** of advertiser spend was lost in an "*unknown delta*" that could not be attributed, representing a third of supply chain costs. The companies who participated in the study were not minor players or fringe organisations; they were all '*blue chip*' companies. The media agency groups include Carat, Mediacom, Mindshare, Wavemaker, OMD, PHD and Zenith Media. The adtech firms include Amobee, The Trade Desk, Google's DV360, Pubmatic, Open X and Rubicon. The publishers include Bauer Media Group, News UK, Telegraph, The Guardian and Autotrader. As a result of this the Incorporated Society of British Advertisers (ISBA) called for the immediate creation of a cross-industry taskforce to uncover the causes of the "unknown delta" and urgent standardisation across contractual and technological areas for more data sharing and transparency.

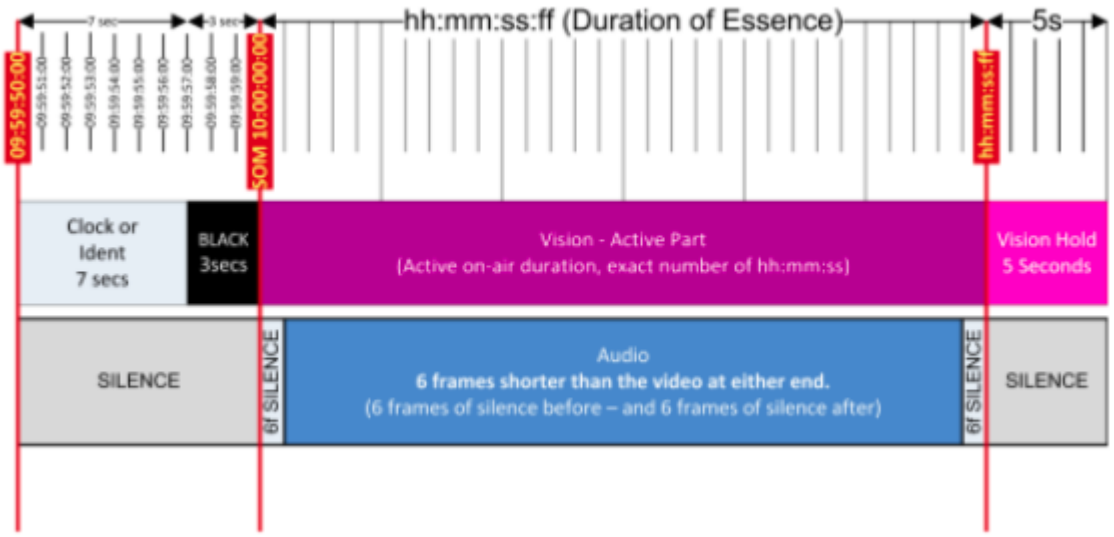
The fact that only **12%** of addressable advertising transactions could be traced through the system should not have come as a surprise to anyone who looked at the Clearcast Clock

Number system in detail (see below) and how it generates money which should be subject to Criminal Finances Act investigations.

"Clocking it"

In broadcast television in the UK every advertisement shown has a "*Clock-Number*" which is used to identify and track payments associated with the advertisement and the advertising campaign. Additionally every advertisement broadcast on the UK commercial television channels is required by Ofcom to be pre-approved before it is broadcast to television viewers. The pre-approval of advertisements is undertaken by a Non Government Organisation (NGO) called Clearcast which was originally set up by ITV in association with other commercial television companies.

The format of an video advertisement for showing on UK broadcast television is as follows (graphic below is taken from Page 16 of the official document at HDCommercialsSponsorshipMaterialStandardITV.pdf :



The problem is that the Clearcast *Clock Number* identifier, for historic reasons, is based upon the premise that a video advertisement is the **same** advertisement being shown to thousands or millions of viewers across a broadcast region (e.g. Grampian) or an entire nation. Hence the Clock Number identifier does not have the granularity to enable it to be

used as an identifier in addressable advertising so that the results are trackable, auditable and fraud resistant.

One solution to this problem would be for the existing Clock Number identification system to be phased out and replaced by an *enhanced* Clock Number identifier system which contained an extension that would enable there to be thousands of "*daughters*" of a Clock Number. Any revised system would need to be backwards compatible because the identification systems will need to run in parallel for many decades if not indefinitely.

Clearcast currently describes its Clock Number system at the following link:
https://kb.clearcast.co.uk/wiki/32/what-is-a-clock-number

The format of a Clock Number is: **AAA/BBBB123/456**

- AAA - is a three letter alphanumeric agency code given to an agency by Clearcast when it registers with Clearcast
- BBBB123 - four letters followed by three numbers. This section is created by the ad agency
- The last 3 digits are the duration of the ad so for example a 30 sec ad will be '030'

The Clearcast identification system has serious size limitations. There are 27 alphabets A-Z in English (if a null or space character is valid) and 10 numeric decimal digits (0-9). Upper and lower case letters are treated the same in the Clearcast system and cannot be distinguished. Thus, when pooled together, there are only 37 alphanumeric characters which can be used in the Clearcast identification system. It is thus possible to uniquely identify only 7,700 agencies

$$37C_3 = \frac{37X36X35}{3X2X1} = 7{,}700$$

7,700 advertising agencies is too restrictive a number for a system which needs to be global and is always open to new market entrants under Ofcom and the UK Competition and Market Authority's (CMA) core regulatory requirements.

Second, when the equivalent calculation is made in respect of the middle field, the number of advertisements from any one agency, this shows that every ad agency has an upper limit of just over 66 Million advertisements that it can uniquely identify during its entire existence. This is clearly too low a number for an addressable advertising system when a single existing Clock Number might be the "*parent*" of thousands of "*daughter*" addressable advertisements, each of which needs to be trackable, auditable and fraud resistant.

Back in July 2021 when my company, SafeCast Limited joined the C2PA[6] I spoke to the Chair of their Threats Work Group (TWG), Leonard Rosenthol, and suggested that I set up an unofficial team which could look into ways in which the security architecture being developed by the C2PA to deal with fake news could be deployed to address the problem of fake advertising. Leonard agreed to this "skunk works project" and I therefore created a small team consisting of people from Microsoft, BBC Research, Adobe, Truepic to whom I circulated a paper with the less than thrilling title "*Paper on Trust List issues to enable the C2PA architecture to be deployed in addressing "fake advertising", fraud and money laundering*" I started considering whether this might be something which could involve support from the OSDI. (OSDI is a project funded by the Government with over £2m in resources to address some of the key challenges around Online Safety data.) I thought that a broad interpretation of their remit could cover a grant towards addressing the problem of "fake advertising". However my skunk works project led to the identification of an immediate solution by the late **Dr Janos Farkas**[7], a Hungarian engineer living in Austin, Texas. In October 2021 Janos suggested that it would be possible to implement Handle as the identifier system - see. http://www.handle.net/tech_manual/HN_Tech_Manual_9.pdf

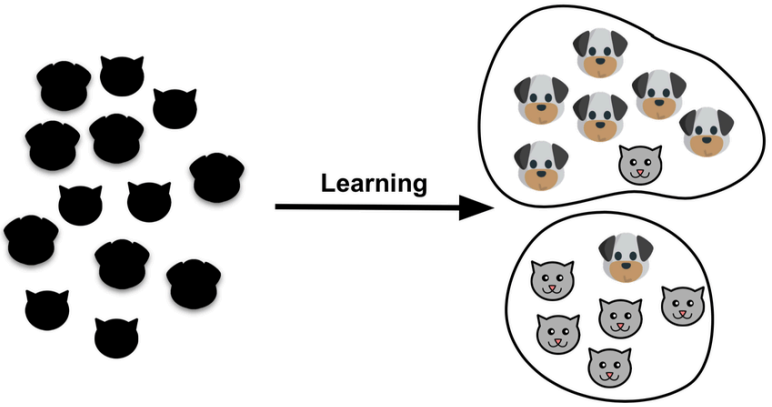
The Handle.Net Registry (HNR), is run by Corporation for National Research Initiatives (CNRI). CNRI is a Multi-Primary Administrator (MPA) of the Global Handle Registry (GHR), authorised by the DONA Foundation to allot prefixes to users of the Handle System. The DONA Foundation is a non-profit organisation based in Geneva that has taken over responsibility for the evolution of CNRI's Digital Object (DO) Architecture including outreach around the world. One of the Foundation's responsibilities is to administer and maintain the overall operation of the GHR, a task that was previously performed by CNRI..

Following on from this work my US Associate, Andy Rosen, in February 2022 wrote a paper on how the American AD-Id labelling system could be deployed in the UK as a solution to these issues which would make use of the Handle Net Registry. This paper remains commercially confidential but I would be prepared to ask him to share it with named reviewers upon request. His paper outlines how global metadata labelling in advertising could be quickly deployed in accordance with a universal standard, thereby reducing the incidence of fraud and crime identified by the ISBA PwC Report and in other studies and reports about organised crime offenders.

[6] At the suggestion of Jatin Aythora, the Chief Architect of the BBC

[7] Who sadly died of COVID in November 2021

Clearcast's failed attempt at retaining its Clock Number as a unique identifier



I understand that, within the past four years Clearcast, which is controlled by Sky (now part of Comcast Inc), failed to implement a conventional bookkeeping *alla veneziana* accounting standard to regulate addressable advertising but instead attempted to retain its Clock Number system as a form of unique identifier through use of Artificial Intelligence (AI). Clearcast's intention was that AI would look at the stream of addressable advertising "*daughter*" advertisements and would automatically assign each of them to its parent using some "secret sauce" from an AI service - thereby avoiding a transition to a new numbering system. It was only later on that this *"solution"* was found not to work. The Clock Number system continues in its 1960s format to this day. As a result serious harm has arisen because, according to independent reports, the lack of granularity in addressable advertising is being used to enable "*click fraud*" by organised crime and is being used to fund terrorism through fake advertising. It is thus a matter for urgent action by the Government.

I would be happy to expand on any of the above matters should this be asked of me.

Alistair Kelman
9 Nov 2022