WHITE PAPER ON
SOCIAL MEDIA “AUDITORS”

by
Street Video Reviewer
hello@streetvideoreviewer.com

July 2024

The police service has a duty to respond to every incident in the appropriate way, first time every time and at every level. A proactive response prevents a significant loss of confidence in the police.

from College of Policing APP on Critical incident management (2013)

When it comes to the police, their powers are certainly not illusory but they do have boundaries. Again however most people do not know where these boundaries lie, or are fearful of crossing them. Therefore they respond with submission to all police requests and this is one of the things that baiters seek to highlight, to — as mentioned before — 'open people's eyes to their rights'. We see this time and time again in the authority baiting videos. It can also be seen in many videos suggested by YouTube as related content that we cannot classify as deliberate baiting but feature people stopped by the police who then film the incident. Police invariably request information (such as a driver's licence or the name and address of the driver) and may even make demands on behaviour (such as 'get out of the car' or 'stand up against the wall') and the person involved refuses on principle because they 'know their rights'. This changes when an arrest is made and it does become incumbent on an individual to supply their details but this also involves the police taking on additional responsibilities too (a duty of care and making the reasons for the arrest clear). It is clear from the surprised reaction of the police that the default reaction to their requests among most members of the public is obedience.

From *Authority baiting as art: On patrol with the Love Police*, by Thomas Chesney (2017)

WHITE PAPER ON SOCIAL MEDIA "AUDITORS"

CONTENTS

Executive Summary 4

Author's Note 5

Introduction 6

Overview 7

1. A brief history of Social Media "Auditing" 10

2. The true nature and purpose of Social Media "Auditing" 15

3. Social media "auditors" and the law 21

4. Business reactions to social media "auditors" 24

5. The digital landscape 27

6. The police response to Social Media "Auditing" 30

7. Civic, social and personal harms of Social Media "Auditing" 37

8. The need for a strategic approach 40

9. Laws and Powers 41

10. Addressing common objections to enforcement 43

11. Conclusions 48

Appendices:

I. "Auditing" methods and blueprints

II. Copy of letter to the ICO, dated 15th. May 2024

III. A list of social media "auditors" as at July 2024

IV. Proposed draft Model Force Policy On Social Media "Auditors"

EXECUTIVE SUMMARY

The core idea behind this paper

Social media “auditing” is an unlawful and anti-social activity, not a type of public photography or vlogging. Given the public nature of “auditing” activity, especially that footage is broadcast on social media, incidences of “auditing” may be considered ‘Critical Incidents’, as defined in the College of Policing APP on Critical incident management (2013).

What this paper does

The 2013 APP on Critical incident management refers to “Three phases of critical incident management”. This paper addresses and seeks to inform Phases 1 and 2 – respectively, preparing for and managing critical incidents – as they may apply to “auditing” and seeks to provide a summary of the problem, explaining why it is a problem and proposing a change in the relevant police policies concerning how officers should respond to the activity.

The aim of this paper

This paper is intended to persuade policymakers to review and change police policies so that a clear distinction is made between public photography and vlogging, on the one hand, and social media “auditing” on the other, with the aim of encouraging the appropriate policing response to the activity, wherever it takes place.

Why this paper has been written

A change in policy may assist response officers, PCSOs, police staff and others to deal effectively with incidents involving social media “auditors”, both on police premises and on commercial and public premises where officers are called to attend. It is hoped a shift in policy may contribute to discouraging and deterring the activity.

What this paper asks the police to do

This paper asks that the National Police Chiefs’ Council and the various police forces agree and promulgate a national policy on social media “auditing” - emphasising its separateness from public photography and vlogging - and to assist officers and others by identifying the relevant criminal offences involved in the activity.

AUTHOR'S NOTE

This paper was written in July 2024.

The law, as stated herein, is for England & Wales and is current as at July 2024. Inevitably only a summary can be provided of the relevant law, and coverage of the law here is not necessarily exhaustive. Mistakes and omissions are the responsibility of the author alone.

The author runs a YouTube channel called Street Video Reviewer (@streetvideoreviewer on YouTube)[1]. The purpose of the channel is to review and critique the content of "auditors", and inevitably the author's assessment of "auditing" content is on the whole negative. For the purpose of full transparency, the author wishes to disclose that a YouTube "auditor" called Marti Blagborough[2] has responded to the author's channel by doxing and harassing the author and posting content that reveals privileged and confidential personal information about the author. Complaints have been made to YouTube about this, but mostly to no avail.

In the interests of brevity, the male pronoun is used throughout for generic purposes. No offence is intended to readers who identify by other pronouns.

[1] Link to channel on YouTube: https://www.youtube.com/@streetvideoreviewer
[2] Link to channel on YouTube: https://www.youtube.com/@MartiBlagborough

INTRODUCTION

The “auditing” trend will be familiar to police officers, but it appears that forces are treating this activity as a type of public photography/vlogging rather than an activity distinct from public photography/vlogging.

The author submits that social media “auditing” should be treated as a discrete activity in its own right, quite distinct and different from public photography/vlogging, and that incidences of “auditing” should be regarded as Critical Incidents (or potentially so) for policing purposes[3]. It is the author’s argument that “auditors” are driven by financial motivations to provoke confrontation with the people they target. They pose as photographers or vloggers not because they genuinely wish to ‘test’ understanding of, or promote or enforce, public photography rights, but in the belief that association with this cause will give their activity the appearance of a legitimate pretext.

The author of this paper is an amateur street photographer[4] who developed concerns about the “auditing” trend and has spent more than a year compiling evidence of the activities of “auditors” on his YouTube channel, Street Video Reviewer (@streetvideoreviewer)[5]. This has consisted in the main of video content in which the activities of “auditors” are analysed in detail from a legal perspective[6]. That content, and the content of auditors’ own channels[7], affords ample evidence that social media “auditing” is inherently unlawful and anti-social in nature. Whether it takes place at commercial and industrial premises or at public and civic buildings, “auditing” consistently involves the abuse and bullying of innocent people (both in person and by electronic mobbing) and is often contrary to the criminal law. It is not a simple exercise of public photography rights, and any policy stance that treats it as such cannot assist in the fair and efficient application of the law by police officers and may, furthermore, contribute to undermining public confidence in the police.

The aim of this paper is to persuade forces and other decision-makers to review and amend their published policies and practices so as to assist and inform those response officers, PCSOs and police staff who may encounter and have to deal with social media “auditors”.

---

[3] As defined in the College of Policing APP on Critical incident management (2013).
[4] Link to the author’s own photography channel on YouTube:
https://www.youtube.com/@streetvideomaker
[5] https://www.youtube.com/@streetvideoreviewer
[6] See these examples from Street Video Reviewer:
Marti Wins Nuisance Money
https://www.youtube.com/watch?v=YWDmFc1C1pg
The Laughing Auditor Got What He Needed
https://www.youtube.com/watch?v=1JB7OMnGlKI
[7] Browse, for instance, the content of DJ Audits: https://www.youtube.com/@DJAUDITS/videos

While there have been isolated efforts to enforce the law against social media "auditors" and even prosecute them in the criminal courts[8], this is not the typical approach of forces and their officers. Too often, we have seen incidents in which officers have applied the law incorrectly or misused their powers[9]; some officers have inappropriately taken a conciliatory, even friendly, approach to auditors when escalation and formal action was warranted[10], no doubt taking the 'line of least resistance'. It is the view of the author that this confusion, ineffectiveness, and misapplication of the law can be attributed to a lack of any strategic approach to the trend and a misunderstanding of what social media "auditing" is and involves, which has encouraged a tendency to class "auditors" as simple vloggers or photographers, albeit carrying out their 'hobby' in a provocative manner. This, in turn, leaves response officers without the knowledge, conceptual framework, understanding, language, procedures and protocols to understand the concerns of victims and the wider public and deal with auditors effectively.

Nobody is suggesting that "auditors" should be arrested or reported for summons on every complaint or encounter. What is suggested is that the general goal of police should be to deter and disrupt the activity, and where the law permits, apprehend the offender. For this to happen, social media "auditors" must first be distinguished as a separate group to photographers and vloggers and their activities must be understood.

[8] Marti Blagborough, for instance, has received at least two Criminal Behaviour Orders in his time in relation to his "auditing" activity. See this video from Street Video Reviewer:
How Auditors Will Beaten
https://www.youtube.com/watch?v=wwpOUFOJya0

[9] See for example this video from Eye Spy Audit:
Unlawfully Arrested For Using £20 Coin
https://www.youtube.com/watch?v=1Xg05vyKbeI

[10] See for instance this video from Street Video Reviewer:
Shame On You, Auditing Britain!
https://www.youtube.com/watch?v=TAZAPkl0RDc&t=22s

OVERVIEW

About the author

The author operates a YouTube channel called Street Video Reviewer (@streetvideoreviewer on YouTube)[11], which provides a mixture of humour, parody and serious and informed legal commentary of the work of vloggers, mainly social media "auditors". This paper distils all knowledge of the "auditing" trend gained by the author from months of careful and close analysis of hundreds of hours of YouTube content uploaded by "auditors"[12] and presents the reality of what the trend is and what "auditors" do.

What is a 'White Paper'?

Outside government circles (especially Whitehall), the concept of a 'white paper' is more familiar to marketing and technical writing. The purpose of a white paper in submissions to policymakers is to make the case for a change in the policy and strategic approach of a public body on an important matter.

What is 'Social Media "Auditing"'?

Social media "auditors"[13] in this context are social media content creators who film around city centres, industrial estates and business parks, business premises, and sites of interest such as police stations and civic buildings. They call themselves 'auditors' because their ostensible stated aim is to test official and public understanding of public photography laws amongst police officers, security staff, workers and others. They upload footage of these encounters to YouTube and other social media platforms.

In reality, the aim of these so-called "auditors" is to escalate these encounters into hostile stand-offs or arguments by provoking the individuals they meet into confrontation[14]. This in turn serves to entertain and rile up their online followers, which generates social media engagement and, where possible, YouTube advertising revenue for the "auditors"[15].

This activity raises wider public concerns because, amongst other reasons:

---

[11] https://www.youtube.com/@streetvideoreviewer

[12] The videos of Street Video Reviewer can be viewed here: https://www.youtube.com/@streetvideoreviewer/videos

[13] The expression "social media auditors" and "auditing" are used by the National Protective Security Authority in their guidance on the trend: https://www.npsa.gov.uk/social-media-auditors

[14] See for instance these videos in which DJ Audits is shown provoking and assaulting a security guard: https://www.youtube.com/watch?v=0km-3FRs9zg https://www.youtube.com/watch?v=r_2f6xTb8sA

[15] See the Street Video Reviewer playlist, *Auditors: The Money Shots*: https://www.youtube.com/watch?v=xDrWtBJH3Hs&list=PLVNCkW0EZUy5SCORm3xcHrQmcmjxm0QeM

- It is a systemised, co-ordinated and organised trend and consists of its own sub-culture, involving photographic techniques, social engineering practices, a shared lingo, and pseudo-legal terminology and concepts that are unique to it.

- As well as the commission of civil wrongs, the activity frequently involves acts contrary to the criminal law.

- "Auditors" never blur out the faces of people in their recordings, and given that the visits take place at people's workplaces, this means that any individual captured in "auditing content" has been identified[16] and had their privacy infringed without justification[17] – and often even without their knowledge, since "auditors" usually do not explain where the footage is going and usually refuse to disclose this when asked[18].

- Police officers are regularly called out in response to incidents involving "auditors" and, in general, seem unable to deal with the problem effectively beyond simple de-escalation[19].

- YouTube have failed to take steps to deal with the trend and put a stop to it, despite the great reliance of "auditors" on that digital platform for earning income from the activity.

Scope of social media "auditing"

Note that social media "auditing" is not confined to YouTube. "Auditors" also have monetised accounts on other third party video content platforms such as Rumble and Odysee, and are also found on Facebook. For the purpose of brevity, the author's focus is on YouTube, but what is said here should also be generally taken to apply to other social media platforms (allowing for obvious shifts in context and differences in terminology and detailed practices between platforms).

---

[16] The definition of 'processing' in Article 4(1) of the UK GDPR (this definition and other aspects of data protection also inform general privacy law in England & Wales):
'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

[17] It is rare that any journalistic justification can be advanced for an "auditing" visit. Article 6(1)(f) of the UK GDPR permits non-consensual processing of personal data on the basis of a "legitimate interest", which can include earning money on YouTube, but this legitimate interest cannot be overridden by the rights of the data subject and those rights must be weighed by the "auditor" in any assessment of the lawfulness of (continued) processing of personal data.

[18] This is a breach of Article 13 of the UK GDPR, which requires the "auditor" as a data controller to provide data subjects with certain information, including who they are.

[19] For another example of police de-escalation, see the video at this link:
https://www.youtube.com/watch?v=2cZCvKV6S7g

1. A brief history of Social Media "Auditing"

In the wake of the 7/7 terrorist attacks in London, it was widely noted that police and private security staff across the country, but especially in London itself, were challenging photographers, especially outside major public landmarks but often even in less sensitive public places[20]. In addition, a growing view emerged that the police were misusing their 'stop and search' powers against photographers and vloggers, especially the power that still existed at that time under section 44 of the Terrorism Act 2000[21], and a new power introduced as section 58A of the Terrorism Act 2000[22].

This situation caused growing disquiet amongst photographers[23] and an informal movement arose to reassert public photography rights[24]. Amongst other activities, this would often involve purposefully attending a public or commercial building and photographing it in full view of security with the aim of asserting the right to photograph and film in public[25]. Many of these photographers would record their activities and upload the recordings to social media, especially YouTube. This type of content proved especially popular where the photographer had recorded himself being confronted in an aggressive manner by staff or security and often the police. This online trend continued for some years, beginning in the late 2000s[26].

Parallel with this, Britain and other Western countries saw a growth in a type of real world radical political and social dissidence fuelled by internet culture. In a short 2017 paper[27], Professor Thomas Chesney of Nottingham University Business School, coined the term "authority baiting" to describe online dissident content, especially on YouTube, that is broadly derivative of the cinéma vérité style[28], essentially performative in nature, and constructed around the theme of a filmmaker questioning an authority figure. A leading personality in this movement was Charles Veitch[29], now associated with the "auditing" trend (though his content is broaden than just "auditing" videos).

---

[20] Is it a crime to take pictures?
http://news.bbc.co.uk/1/hi/uk/7888301.stm

[21] Photographers snap over use of Section 44 by police officers:
https://www.independent.co.uk/news/uk/home-news/photographers-snap-over-use-of-section-44-by-police-officers-1833839.html

[22] Photographers fear they are target of new terror law:
https://www.theguardian.com/media/2009/feb/12/photographers-anti-terror-laws

[23] *Paranoia and suspicion: photographers are not terrorists:*
https://blog.mingthein.com/2015/03/02/paranoia-and-suspicion-photographers-are-not-terrorists/

[24] https://phnat.org/

[25] For example, see this video called *Stand Your Ground*:
https://www.youtube.com/watch?v=FJH9F7Hcluo&t=59s

[26] An early exponent of this was Happy TV, whose content seems to span legitimate photography/vlogging and "auditing": https://www.youtube.com/@HappyTVHappyTV

[27] *Chesney, T. (2017). Authority baiting as art: On patrol with the Love Police. First Monday, 22(12):*
https://firstmonday.org/ojs/index.php/fm/article/view/7122/6584

[28] https://en.wikipedia.org/wiki/Cin%C3%A9ma_v%C3%A9rit%C3%A9

[29] https://www.youtube.com/@CharlesVeitch

The photographic protest trend lost some of its impetus with the suspension and repeal of Section 44 in 2010, which took a lot of the sting out of criticisms of the police. Nevertheless, the trend continued to grow and had wider appeal than just photographers. The content was also liked by people who were not photographers and may not have even felt very strongly about the underlying issues involved but nonetheless found it entertaining to see police and private security personnel confronted and entrapped in "gotcha" situations. This is because it is easy to make petty authority figures look ignorant, clumsy, overbearing and foolish on camera, as the nature of their duties involves having to question people who may turn out to be doing absolutely nothing wrong[30], and in the wider online climate of increasing cynicism about authority and a growing trend for 'authority baiting'[31], this content took off in popularity.

It dawned on some people that this sort of 'authority baiting' content may have the potential to be lucratively monetised on the YouTube platform. In around 2014/15, a new noticeable trend emerged in which content creators who were not necessarily photographers - and may have had scant or little understanding of photography or sympathy for the rights of photographers - began attending at various buildings to continuous film and provoke a reaction from the occupants. Often the people caught in the recordings were private security guards, and any police officers called out in response, but there was especial interest in filming police stations and other police premises, and while the ploy was not exclusively aimed at the police, the bulk of this early content targeted officers[32].

Some of these early content creators must have regarded this type of content as an opportunity to earn income and perhaps also kudos. Others may have been motivated more by certain social and political beliefs, perhaps a vestige of earlier arguments against police overreach under the anti-terrorist legislation. Still others may have harboured a general spiteful dislike of the law or authority.

Concomitant to this, an online social media movement had arisen in the United States in which people calling themselves "auditors" or "First Amendment auditors" or "Fourth Amendment auditors" would go round continuously filming themselves walking into public buildings or private businesses to confront the occupants - businesses, police or public officials, or whatever[33]. These confrontations would then be broadcast on YouTube. The

---

[30] A classic video from the period was the Golden Wonder security incident: https://www.youtube.com/watch?v=BjTBYdJwQ4I

[31] Ibid

[32] One of the earliest examples of this was Auditing Britain, who began uploading "auditing" videos during 2015. His very first "auditing" video, in 2015, targeted security guards in his hometown of Banbury: https://www.youtube.com/watch?v=pZYN02SDRjM

[33] A prominent American "auditor" is Amagansett Press: https://www.youtube.com/@AmagansettPress/featured

US “auditing” movement, in fact, dates back to at least as early as the 1990s, when activists in America would undertake this activity to supposedly assert their constitutional rights, but until the popularisation of social media, it was an extremely marginal and obscure activity. Due to YouTube and Facebook, American “auditors” were suddenly able to build up mass followings and committed supporters, and the number of “auditors” multiplied as awareness spread and some viewers decided to start their own “auditing” channels[34].

There were important differences between the American and British trends. The American trend[35] was more aggressive and less rooted in photography than its UK counterpart, but the UK content creators quickly noticed what was happening in the United States and started to ape the more aggressive tactics, methods and styles, dress and pseudo-legal lingo and terminology of the Americans[36]. Most importantly, the UK content creators started calling themselves “auditors”[37]. This cross-pollination resulted in some of the most fundamental misunderstandings that linger to this day amongst UK auditors about the laws applicable to their activity. To give one example: it is common for U.S. auditors to enter premises and refuse to leave on the basis that the premises are accessible and there are no signs prohibiting entry. It could be that this behaviour is condonable in law in some parts of the United States, but under English law, the general position is that anyone who unlawfully interferes with land is a trespasser, regardless of whether there are signs or the land or building is accessible to the public. Despite this, UK auditors have borrowed the tactic from the United States and still frequently argue that they have an “implied right” to be in or on premises on the basis that it is accessible[38].

“Auditing” in the UK (as well as the United States) was given renewed impetus due to the imposition of the Covid-19 public health restrictions, especially lockdowns. “Auditing” viewer numbers massively increased during the period 2020-2022, coinciding with much of the population being furloughed or working from home, and some “auditors” used the conduct of the police during the Covid-19 pandemic as a pretext to adopt abusive and aggressive methods. “Auditing” is now at its peak in terms of viewer numbers and subscribers on YouTube. It has never been more popular. It is likely that

---

[34] An American “auditing” channel created in 2021, Long Island Audit, has amassed 782,000 subscribers as at 25th. July 2024.

[35] See this commentary from an American attorney on “auditing” in the United States:
First Amendment Auditors Are Crazy
https://www.youtube.com/watch?v=W0hHPcgFchA&sttick=0

[36] To the extent that some UK auditors even started using American legal terminology and making reference to their “First Amendment” rights and “First Amendment audits”, despite being in the UK.

[37] Probably the American “auditor” who influenced the UK scene the most was Amagansett Press – see note 33 above.

[38] For further elucidation, see the Trespass for Dummies series on Street Video Reviewer:
https://www.youtube.com/playlist?list=PLVNCkW0EZUy5hcrUfUqevY0ovw7g3ivCe
See also the Street Video Reviewer playlist on section 33 of the Criminal Justice Act 1972:
https://www.youtube.com/watch?v=WT6n9N6wIXM&list=PLVNCkW0EZUy4k5OCF3xQ26nemWcNPvQ7o

Covid-19 accelerated awareness of “auditing” and that without the pandemic, the growth in viewer numbers would have been slower.

What we now call “auditing” has lost any sense of the original purpose of the pioneer photographer-activists back in the late 2000s, who were protesting what they perceived to be police and security abuses of actual photographers. “Auditors” frequently behave unpleasantly towards their targets[39], often commit civil wrongs such as trespass[40], are not compliant with data protection laws and regulations[41], and often act contrary to the criminal law[42]. They seek to provoke confrontation in order to gain views and income from YouTube[43]. Furthermore, “auditing” is an astro-turf trend[44]. “Auditors” claim to be upholding public photography rights, but these claims are belied by their own obnoxious (and frequently unlawful) behaviour, and the explosion in social media over the last decade: there are millions of legitimate photography and vlogging channels on YouTube in which content creators photograph and vlog in public without reporting any significantly problems or difficulties at all with the law, or security staff, or anyone else, or if and when they do, they choose not to turn it into a regular feature of their content in its own right[45].

The global geographic spread of “auditing”

“Auditing” is in the main an Anglophone phenomenon. It does exist outside the Anglophone world, but as a much smaller phenomenon. This may be because the more aggressive style of “auditing” that a certain type of person finds entertaining is associated with the United States, an English-speaking country, thus its influence is mainly in other English-speaking countries.

---

[39] For examples, see the Street Video Reviewer playlist on Marti Blagborough:
https://www.youtube.com/watch?v=sHI6uNYcIRc&list=PLVNCkW0EZUy6s9oecllwnW9ssEe0rv3Qz

[40] n 38

[41] See the Street Video Reviewer playlist on data protection:
https://www.youtube.com/watch?v=LJN6GbBpMmo&list=PLVNCkW0EZUy79YE_7ph8CD7n-d96gKzux

[42] See the following selection of videos from Marti Blagborough:
https://www.youtube.com/watch?v=RDD55Gjd_bw
https://www.youtube.com/watch?v=W0lT3cCNPzY
https://www.youtube.com/watch?v=LX8VecSsBcQ

[43] See n 15 and also the following content from Street Video Reviewer:
Watch UK Meet The Tyrants Get What Was Coming To Him
https://www.youtube.com/watch?v=jRuMwGrkgxQ&t=55s
UK Meet The Tyrants Gets Another Belting
https://www.youtube.com/watch?v=22_ixvms1xM&t=20s
Right Bankers
https://www.youtube.com/watch?v=kazQSVW-XVA&t=34s

[44] See the Street Video Reviewer video, *"Photography Is Not A Crime" - Is That Always True?*
https://www.youtube.com/watch?v=F4uuF_WR48o

[45] See from Street Video Reviewer:
Why Doesn't Macc Man Have The Same Problems As DJ Audits?
https://www.youtube.com/watch?v=SIGdLeFzWOo

Another factor may be reasons of legal sociology. Countries such as Britain, the United States, Canada, Australia and New Zealand, all have mainly common law legal systems with heavily influential traditions of political liberalism in which freedoms such as public photography are strongly upheld by the courts, police and legislatures. The downside of this is that it may leave the authorities blindsided when, as with “auditing”, a trend emerges in which established rights and liberties are being used to abuse people.

By contrast, countries influenced by Napoleonic systems of law may place greater emphasis on restrictions based on privacy rights and so on, with the authorities more ready to crackdown on abuses – with the downside that innocent and genuine photographers and vloggers may have less room for free expression of their art and creativity.

2. The true nature and purpose of Social Media "Auditing"

Social media "auditing" is not photography[46]. It is an unlawful activity[47] in which a social media content creator acts in a calculated manner by setting out to engineer a conflict with police officers, security staff or just ordinary innocent workers for the entertainment and gratification of viewers. Obscure and mundane commercial and industrial premises – warehouses, factories, offices, and the like – are targeted in the knowledge that staff will invariably seek to question the "auditor" about why he has turned up to film comings and goings at the premises.

The auditor will often be masked[48] and will behave in a conspicuously odd, intrusive or obnoxious manner to attract attention and encourage a challenge and confrontation with a staff member. He may commit trespass[49]. He may taunt and insult staff. He will never blur out faces in recordings[50], which means that innocent staff members are identified on YouTube, often without their knowledge as the "auditor" will usually refuse to explain what the purpose the exercise serves and what will be done with the footage. This is a clear infringement of privacy and breach of data protection[51], for which there is rarely any justification[52].

Genuine photographers and vloggers do not behave in this way[53]. There are millions of photography and vlogging channels on YouTube in which the content creator can happily go round filming in public and rarely face any difficulty or objection[54]. This suggests that it is primarily the behaviour of "auditors" that provokes the objections to "auditing", rather than the activity of photography in itself.

Tactics of auditors

To summarise, typical tactics of "auditors" include:

---

[46] For a detailed discourse on this topic, see this video from Street Video Reviewer:
Auditors & The Street Photography of Bruce Gilden
https://www.youtube.com/watch?v=9wrd0F1Am3o

[47] For a summary of the law relating to "auditing", see section 3 below.

[48] See the following short from Street Video Reviewer:
What Would You Do?
https://www.youtube.com/shorts/FuMg2rOdV6k

[49] n 38

[50] The blurring of faces in Street Video Reviewer content has been added by the author, it is not native to the content of any of the "auditing" channels.

[51] n 16, 17, 18 & 41

[52] n 17

[53] n 45 & 46

[54] n 45

- *Conspicuously filming* premises, staff, customers/clients, and other visitors, so as to provoke a challenge from staff, that can then be filmed[55].

- *Provoking staff*, by attending reception, or shouting insults or taunts at staff, or trespassing, behaviours intended to provoke a response that will entertain viewers (the initial provocation is, of course, edited out of the uploaded video)[56].

- *Claim grifting*, in which the "auditor" acts in such a way as to provoke the police to use their powers of arrest, detention or stop and search and then instructs solicitors to initiate a claim for compensation from the relevant force, typically on the basis of some minor procedural or technical irregularity in the use of police powers. Force legal departments have settled claims with "auditors" and awarded them thousands of pounds of public money in circumstances where the error by officers was purely a technicality, or even where it is unclear what exactly officers did wrong[57].

- *Posing as a "member of the public" or innocent photographer/vlogger*, while not revealing the true purpose of the visit or that the footage will be uploaded to social media later[58].

- *Exaggeration of purpose*, for example by the auditor telling the occupier that he is carrying out some sort of official "inspection"[59].

---

[55] For examples of this tactic, see any of the content from DJ Audits and BP Visits., both on YouTube.
[56] As an example, see this content from Marti Blagborough:
Stupid Police at Heckmondwike Police Station. Audit
https://www.youtube.com/watch?v=hq7xy7s1TYA
[57] See for example see this content from Marti Blagborough:
SGT Sausage Orders my Arrest for Filming a Police Station
https://www.youtube.com/watch?v=Q-5dgFLIUw4
See also this content from Street Video Reviewer:
Marti Wins Nuisance Money
https://www.youtube.com/watch?v=YWDmFc1C1pg
See this content from Auditing Yorkshire, in which he turns up at a public building masked and filming and behaves in a insulting and provocative manner and is rightly arrested for a public order offence, but later claims he was compensated by the police and the arresting officer lost his job as a result:
Inspector Dyson Retires From The Police Force!
https://www.youtube.com/watch?v=yRZpXkiN4Fg
Arrest video from body worn camera of the inspector:
https://www.youtube.com/watch?v=YggD5fqzXhI
[58] See this content from Street Video Reveiwer:
Trespass for Dummies, Part 1 - With Ace Audits
https://www.youtube.com/watch?v=acuoNE39b2g
[59] For examples of this ploy, see the following "auditor" content:
https://www.youtube.com/watch?v=k2a3S7gfvhU
https://www.youtube.com/watch?v=_bk1B3dbjSA
https://www.youtube.com/watch?v=JTpGS8hrsj8

- *Covert filming*, in which the "auditor" does not disclose to staff that he is still filming or filming at all. The "auditor" may be conspicuous about filming at first, then affect to stop filming while another camera remains switched on and records what is happening[60].

- *Decontextualisation*, taking the form of commenting on, and even interfering in, stop and searches as they happen nearby, while vocally provoking and taunting the officers in attendance and portraying the officers as abusing their powers[61].

- *Provocation with a drone*, in which the auditor films himself informing an occupier that he intends to fly a drone over their premises. This is done to provoke a response in the knowledge that the majority of staff will not have a detailed working knowledge of drone law and may react with alarm or concern at the prospect of a drone flying over their premises (and this concern is often not without justification)[62].

- *Mobbing*, or a mass "audit", in which multiple "auditors" attend at premises together, with the intention of haranguing that business or public body in numbers and adding to the sense of intimidation for the people on the receiving end[63].

- *Silent "audits"* are where an "auditor" stands and films without speaking. A mass silent audit is simply this tactic on a larger scale[64].

- *Harassment*, in which "auditors" co-ordinate multiple visits to the same premises. This is especially common if there is an adverse reaction to an "auditor". If this happens, other "auditors" will then visit those premises as a 'show of support' for the previous "auditor". There have also been occasions when "auditors" have paid repeat visits to premises in order to target particular individuals whom they perceive wronged them on a previous visit[65]. (Note in addition that it could be argued that

---

[60] This is a ploy typically used by DJ Audits.

[61] This tactic is frequently used by Auditing Britain. For a classic example, see this video from his content:
https://www.youtube.com/watch?v=7BlyH-LkT-o

[62] This is a favoured tactic of PJ Audits and DJ Audits.

[63] For an example of a mass "audit", see this video from Marti Blagborough, in which a number of audits (introduced early in the video) harassed Libra Speciality Chemicals Ltd in Irlam, Greater Manchester:
https://www.youtube.com/watch?v=Vdu7rhjWP3E

[64] Examples of some silent "audits":
https://www.youtube.com/watch?v=x2WrcrcfX9Q
https://www.youtube.com/watch?v=erOChujZi-U

[65] See for instance the harassment of a Werst Yorkshire Police inspector by Auditing Yorkshire across several videos – for example:
Inspector Dyson Retires From The Police Force!
https://www.youtube.com/watch?v=yRZpXkiN4Fg

since the "auditing" activity itself involves multiple processing events – visiting and recording in antagonistic circumstances where the individuals can be identified and do not want to be filmed (and may expressly object and/or have not given informed consent), then uploading and broadcasting the results – this amounts to at least two "occasions" of harassment, meeting the criteria in sub-section 7(3)(a) of the Protection from Harassment Act 1997 for a criminal offence contrary to section 2 of that Act).

- *Doxxing*, is in effect a common feature of all "audits" uploaded to YouTube, since "auditors" never blur out faces. "Auditors" also seek to dox their critics online as a form of intimidation and to discourage determined criticism of their activities[66].

- *Humiliation and personal abuse of staff*, which is in the video itself of the majority of "auditing" visits, and also often in video titles and descriptions, in which "auditors" will frequently use personally abusive and insultive language to describe individuals they encounter whom they have not taken a liking to[67].

- *Electronic mobbing*, in which YouTube users who support and follow "auditing" content will add harsh and defamatory criticism of the individuals shown in a video and often call for them to be disciplined or sack by their employers[68].

- *Malicious reviews*, in which supporters of "auditors" leave malicious online reviews for businesses featured in "auditing" content. Sometimes this is done with the encouragement of the relevant "auditor"[69].

See also n 63 above, which was a 'revenge' visit after an auditor had received a negative response from the company. Another example would be the mass "audit" to IPB, a company in the north-east of England:
https://www.youtube.com/watch?v=YBchGEnPeA0&t=214s

[66] Marti Blagborough responded to criticisms on the channel Street Video Reviewer of his activities by doxxing this author.

[67] In a series of videos, Auditing Yorkshire refers to an inspector of West Yorkshire Police as "Inspector Muppet". For example:
Inspector Dyson Retires From The Police Force!
https://www.youtube.com/watch?v=yRZpXkiN4Fg
Auditing Yorkshire harassed a parking enforcement officer in Huddersfield:
Auditing Yorkshire Is The Worst I Have Seen
https://www.youtube.com/watch?v=hxmW_BrdWqQ

[68] There is no need to reference specific evidence of this behaviour, as it can be found beneath virtually any "auditing" video. For examples, look beneath the videos on the larger "auditing" channels.

[69] See for instance the latest Google reviews for Libra Speciality Chemicals Ltd in Irlam, Greater Manchester:
https://www.google.com/search?q=Libra+Speciality+chemicals&sourceid=chrome&ie=UTF-8#lrd=0x487baa486509fed1:0xb29ef7e867014079,1,,,,
Those reviews were left by supporters of "auditors" after the mass audit there (see n 59 above).

- *Simulating suspicious behaviour*, especially around police stations, such as filming inside cars and windows, recording number plates, and similar behaviour, knowing that this is bound to lead to a challenge from a police officer that can then be filmed[70].

- *Simulated hostile reconnaissance*, at police stations and sensitive sites such as important public buildings and around military bases, in which the "auditor" acts in such a way as to arose suspicions that he may be a terrorist, so that he can film a confrontation with police or security or both[71].

"Auditing" as a sub-culture

"Auditors" share a lingo, dress code, and a pseudo-intellectual understanding of the law that makes use of factitious legal concepts and statutory interpretations. These motifs form a sub-culture in which "auditors" exhibit common and consistent norms of delinquent behaviour: they insult everyone who challenge them, they portray police officers, security staff and other authority figures as 'tyrants' and 'bullies' (literally using those words); they frequently trespass on property on the basis of a misconceived belief that if the premises are publicly-accessible, it is not trespass; and, they misquote statutory provisions such as section 33 of the Criminal Justice Act 1972[72]. Their dress code is intended to cause consternation and alarm and involves wearing a mask[73] to conceal their identity and provoke a challenge to their presence. They trample on their victims' privacy and property rights and show no concern for the dignity or feelings of others.

Auditing is not journalism

"Auditing" is not journalism. It may be true that there are examples of photojournalists doing some of the above things and not having regard for privacy, but anyone abused by a journalist or photojournalist has recourse; "auditors" are acting outside the law and in grey areas and their activity is not regulated, nor can it be, since it shows a fundamental disregard for the rights and dignity of others. Auditors frequently dismiss and disregard protests from people captured in their footage that they do not wish to be filmed. Auditors will rarely even disclose to their victims what they are actually doing and where the footage, if uploaded, will appear. Such behaviour is likely to be a

---

[70] See for example this video from Street Video Reviewer:
The Laughing Auditor Got What He Needed
https://www.youtube.com/watch?v=1JB7OMnGlKI

[71] See this video from Street Video Reviewer:
How Auditing Britain Wastes Police Time - And Why It IS A Crime!
https://www.youtube.com/watch?v=ye8Q6X40f0k

[72] See the Section 33 playlist on the Street Video Reviewer channel:
https://www.youtube.com/watch?v=WT6n9N6wIXM&list=PLVNCkW0EZUy4k5OCF3xQ26nemWcNPvQ7o

[73] n 48

source of alarm or distress for victims and the thought of appearing online in footage that will be edited to make the person look foolish or inept must be a source of great worry for many.

It is rare that “auditors” will have a newsworthy purpose or some other public interest justification for a particular visit, and even when potentially they might, their main focus is still to needle and provoke staff into a confrontation, as that is what is watchable for their audience[74].

[74] Only rarely will “auditing” content meet the criteria for ‘journalism’ in the field of data protection law, as set out in Part 5 of Schedule 2 of the Data Protection Act 2018.

3. Social Media "Auditors" and the Law

There is an established common law liberty to photograph on a public right of way, and this includes the liberty to photograph anyone or anything that can be seen from a public right of way, including people and things on private premises, with or without the consent of the owner or occupier or the person(s) being photographed. This liberty is codified in the form of the rights in Article 10 (the right to freedom of expression) and Article 11 (the right to freedom of association) to Schedule 1 of the Human Rights Act; but those rights are subject to law, and can be restricted by law, and do not extend to abusing, exploiting, pestering, annoying and hassling others and, in many cases, behaving in a way that is intended to cause or is likely to cause harassment, alarm or distress. Furthermore, Article 8 codifies a right to a private and family life.

It is important to abundantly emphasise that it is not the author's intention in this paper to any way question or undermine public photography rights. The author is an amateur street photographer himself. Social media "auditing" is not photography or vlogging[75]. It is not journalism[76]. It is not a legal activity[77]. On the author's YouTube channel, Street Video Reviewer[78], can be found detailed legal breakdown and analysis of "auditing" videos[79] in which it is clearly shown that most "auditing" visits involve one or some combination of the following offences (this list not necessarily being exhaustive):

- Public order offences, contrary to sections 4A and 5 of the Public Order Act 1986.

- Harassment, contrary to section 2 of the Protection from Harassment Act 1997. It is arguable that published "auditing" incidents are criminal harassment *per se*, as the criteria in section 7(3)(a)[80] is met simply by the process of the auditor capturing facial images in antagonistic circumstances where the individuals can be identified and do not want to be filmed (and may expressly object and/or have not given informed consent) then posting those images online (often multiple times to the same or different social media platforms), and without any attempt to pseudonymise victims.

- Aggravated trespass, contrary to section 68 of the Criminal Justice and Public Order Act 1994.

---

[75] n 45 & 46

[76] n 74 and pp 19-20 above.

[77] n 44 & 47 and the summary of the relevant law in this section 3.

[78] @streetvideoreviewer on YouTube.

[79] https://www.youtube.com/@streetvideoreviewer/videos

[80] Note that there have been instances of the same "auditor" visiting the same premises on at least one further occasion, but this is uncommon.

- Being found in an enclosed yard for an unlawful purpose, contrary to section 4 of the Vagrancy Act 1824.

- Assault, contrary to section 39 of the Criminal Justice Act 1988.

- Assault by battery, contrary to section 39 of the Criminal Justice Act 1988.

- Communications offences, such as those under section 127 of the Communications Act 2003, section 1(1) of the Malicious Communications Act 1988 and section 179(1) of the Online Safety Act 2023.

- Obstructing a constable, contrary to section 89(2) of the Police Act 1996, by deliberately acting in a suspicious manner to provoke police attention or by simulating hostile reconnaissance activity.

- Taking a photograph in a court building, contrary to section 41 of the Criminal Justice Act 1925.

- Taking a photograph within a prison without authorisation, contrary to section 40D of the Prison Act 1952.

- Eliciting or publishing information likely to be of assistance to a terrorist, contrary to section 58A of the Terrorism Act 2000.

- Entering, inspecting, passing over, etc. a prohibited place for a purpose prejudicial to the safety or interests of the United Kingdom, contrary to section 4(1) of the National Security Act 2023.

- Unauthorised entry to, inspecting, passing over of, etc. a prohibited place, contrary to section 5(1) of the National Security Act 2023.

- Preparatory conduct in relation to the offence in section 4(1), contrary to section 18 of the National Security Act 2023.

- Unlawful obtaining of personal data without the consent of the data controller, contrary to section 170 of the Data Protection Act 2018.

- Offence of causing nuisance or disturbance on NHS premises, contrary to section 119 of the Criminal Justice and Immigration Act 2008.

All of this is in addition to breaches of the peace in which there have been occasions when “auditors” are heard to act or speak in such a way as would put a reasonable person in fear of violence.

While not strictly police matters, the following breaches and infringements of the law are also regularly committed by “auditors”, further demonstrating their disregard for law:

- Breaches of the drone laws and regulations – including criminal offences (for instance, it is common for “auditors” to disregard the Visual Line of Sight requirements). These breaches could be prosecuted by the Civil Aviation Authority (CAA) (sometimes the police will be called on to assist the CAA in these matters).

- Virtually no “auditor” is compliant with data protection[81], and various regulatory breaches of data protection are obvious throughout “auditing” content, including (amongst other things) failure to comply with the disclosure requirements in Article 13 of the UK GDPR[82] and failure to register as a data controller, as required under Regulation 2 of the Data Protection (Charges and Information) Regulations 2018. These failures can attract substantial civil fines, should the Information Commissioner’s Office (ICO) elect to enforce the regulations against “auditors”.

“Auditors” also habitually commit various civil wrongs - typically including trespass of land, aerial trespass (with a drone), trespass to the person, misuse of private information, and individual and corporate harassment. Victims of auditors –individual staff, businesses and companies – could bring civil proceedings in the courts against “auditors”[83].

[81] Auditors collect and process personal data as defined by Article 4 of the UK GDPR. It is well established law that citizen journalism and vlogging content can be caught by data protection. See, for instance the ruling of the European Court of Justice in *Sergejs Buivids c/ Datu valsts inspekcija* [8][8]CCE 2019.

[82] Article 13 of the UK GDPR requires that a data controller identifies himself to a data subject, to include the provision of his name and address, and confirms the purpose of processing and other details.

[83] At least two “auditors”, DJ Audits and DJE Media, are currently the subject of injunctions obtained by HS2, due to their previous activity at, on, above and around HS2 sites. This included an assault of a security guard by DJ Audits at an HS2 site. For further information, go to the links below:
https://www.gov.uk/government/publications/hs2-route-wide-injunction-proceedings-2023
https://www.gov.uk/government/publications/hs2-route-wide-injunction-proceedings-2024

4. Business reactions to social media "auditors"

Risk is the main concern of a business, public body or other organisation that receives a visit from an "auditor". Depending on the nature of what the occupier does on site, the presence of the "auditor" may pose a health and safety risk; there may be a risk to the commercial confidentiality and privacy of the business and its staff, and perhaps also of suppliers or clients and customers of the business; and, there could be a risk to the reputation of the business if unauthorised filming is allowed.

Genuine photographers and vloggers can assist in ameliorating and minimising some of these risks by (amongst other things):

- Providing clear explanations for the nature, scope and purpose of the filming, a risk assessment and flight plan for the drone (if applicable), and confirmation of what will be done with the footage and why, with the provision of contact details should the business wish to complain or object or otherwise exercise its legal rights against the photographer/vlogger.

- Taking steps to protect the privacy of individuals by blurring out their faces during editing of footage and through simple techniques such as pointing the camera away from individuals unless identification is justified, etc.

- Wearing Personal Protective Equipment (PPE) appropriate to site.

- Requesting an induction before walking round site (assuming permission has been granted to enter).

- Having a policy of public liability insurance cover on risk for the photographing/vlogging activity (including any drone being used).

- Explaining any applicable justification where filming is to be carried out without the consent of the occupier, or despite the occupier's objections.

- Refraining from visiting in the first place without obtaining prior permission.

"Auditors", by contrast, rarely or never engage in any of these steps. If an occupier were to permit an "auditor" to enter premises, this would present all sorts of issues for that business or public body or other organisation, including insurance and data protection, amongst many other things. If an accident occurs that results in personal injury to a staff member or customer, or the "auditor" himself, or the wrongful or unlawful disclosure of personal data of a staff member or customer, where is the liability? Is any insurance policy

effective to cover that risk? These and other questions would have to be addressed by a conscientious occupier. There may well be clear answers in law to these questions, but that is not the point. The occupier is being put in a position of having to consider these issues and questions without prior notice of the "auditor's" visit.

Against this background, the common advice now given that occupiers should simply "ignore" "auditors" may work in particular situations, and it will form part of the solution to the problem, but is not a workable solution in general. It is also potentially bad advice from a security point of view.

It does not and cannot work because:

(i). auditing is proactive, not typically reactive. The nature of what auditors do is that they are seeking confrontation with ordinary working people (and officials and police officers, etc.). The auditor needs content, so he will look for ways to provoke a response – if necessary, he will confront the business by going to reception/entrances or accosting staff, in the hope that this will provide content, even if it is just a simple, friendly interaction; and,

(ii). the real basis of auditing is the exploitation and abuse of the normal response of staff to a strange person (often masked[84]) continuously filming business premises while stood on or near the premises. This will include conspicuously filming staff, clients, visitors and operations, and will often also involve deliberately acting in a suspicious manner so as to prompt concerns and encourage an approach and response[85]. It is perfectly normal for staff or security to approach an auditor in those circumstances[86], or report the matter to the police, and auditors know this and exploit it. That is why they have content. In most of these situations, to ask staff not to approach such a person or not alert the police would be odd and counter-intuitive from the point of view of staff.

Ignoring the presence of an auditor is also a bad idea from a security point of view for fairly obvious reasons. Unless it is the sort of premises that attracts curious visitors and tourists, staff should not just ignore somebody filming, and it is commonly the culture in UK workplaces that all staff share responsibility for site security and should challenge and report strange persons. By suggesting that auditors should be ignored, a change in this culture is proposed, which will create new problems. There is simply no way of being sure that the individual is an auditor, and even if he is recognised as someone who resembles a known auditor, staff cannot be expected to rely on that conclusion. Either somebody has to approach the auditor or, if it is believed

[84] n 48

[85] For a discussion of "auditor" tactics, see section 2, pp 15-19 above.

[86] n 13

that the auditor should not be approached, staff should seek advice from the police.

One may add to these observations that some staff may approach “auditors” on purpose in the knowledge they are being filmed, seeing some appeal in the prospect. This, again, is a risk that employers and business owners have to address and manage by, in turn, managing and controlling the interference of “auditors” in the normal lawful site activities.

5. The digital landscape

There are millions of public photography and vlogging channels on YouTube that go about their business in compliance with the law, with few or no challenges to their public photography rights, and with no disruption to other people's lives[87]. By contrast, YouTube frequency receives complaints concerning the content of social media "auditors" and regularly removes such content on the grounds that its various policies[88] and Community Guidelines[89] have been breached by the "auditor": this includes where the content infringes the privacy of others, encourages violence or other criminality, or harasses, bullies or defames others.

"Auditors" upload their content to various social media platforms, of which YouTube is their primary social media platform of choice[90], while other platforms such as Facebook and Tiktok are used to spread awareness of new content uploaded to the "auditor's" main YouTube channel. The general legal position in the UK with regard to harmful or offensive content of the type produced by "auditors" is that YouTube as a third-party video content platform is availed of a 'conditional immunity' in UK law in respect of any civil or criminal liability: specifically, the immunity applies on the condition that YouTube promptly removes any offending content on being notified of it.

YouTube Terms of Service for the UK include this admonishment to content providers:

You are legally responsible for the Content you submit to the Service.[91]

Unfortunately, YouTube will only rarely penalise an "auditor" in any meaningful way and, despite numerous daily breaches by social media "auditors" of data protection law and YouTube's own policies, YouTube rarely actually terminates any "auditing" channel.

The immunity in law enjoyed by YouTube is not absolute and direct liability for content could potentially fall on YouTube itself for the following reasons:

(i). First, where YouTube is aware that certain content creators who are "auditors" are uploading illegal or harmful content, and fails to take further preventative steps to terminate or demonetise those channels, it

---

[87] n 45

[88] YouTube policies: https://www.youtube.com/intl/ALL_uk/howyoutubeworks/policies/overview/ YouTU privacy policies: https://www.youtube.com/intl/ALL_uk/howyoutubeworks/our-commitments/protecting-user-data/#privacy-guidelines

[89] YouTube Community Guidelines: https://www.youtube.com/intl/ALL_uk/howyoutubeworks/policies/community-guidelines/

[90] The other major platforms used by "auditors" are Facebook and Tiktok. TikTok is growing in popularity but YouTube remains the mot important platform.

[91] https://www.youtube.com/static?gl=GB&template=terms

could be argued that a vicarious liability then falls on YouTube for any criminal offences and civil wrongs that result. This is because the harm caused is foreseeable by YouTube under those circumstances.

(ii). Second, and in relation to data protection specifically, it is arguable that Google LLC is joint data controller with the "auditor" of any personal data captured in "auditing" content, because YouTube has decision-making control over that personal data, alongside the "auditor", through its own aforementioned policies and guidelines for content creators. Therefore, YouTube is secondarily (or vicariously) liable for any data protection duties and obligations relating to that content. In normal circumstances, this potential liability would be of little practical relevance or import, but could become relevant in circumstances where it can be shown that there has been a systematic failure on the part of YouTube to prevent breaches of the rights of data subjects by "auditors". This is on the basis that the breaches have become 'foreseeable' in that YouTube is already aware of the actions of "auditors", both collectively and individually

It is important to note that the existing privacy, data and harassment policies and Community Guidelines of Google LLC/YouTube[92] are insufficient to tackle the discrete problem of "auditing" content.

In particular:

(iii). YouTube has insufficient mechanisms to tackle circumvention of its safeguards[93]. "Auditors" routinely re-upload any content removed by YouTube, usually in its original form with no editing whatsoever. When an "auditing" channel is deleted, the user simply starts another channel (often these channels already exist and contain all the "auditor's" content but set to delisted or private, ready to go 'live' in the event the original channel is removed or deleted by YouTube). There is no mechanism for users to specifically report activities by content creators that circumvent YouTube guidelines and policies, and "auditors" routinely get away with these circumvention methods.

(iv). "Auditors" threaten business owners with adverse and negative online reviews from their rabid followers[94] if they stand up to them or challenge them. In this climate, few victims of "auditors" will want to contact "auditors" direct and given the circumvention activities outlined in (iii)

---

[92] n 88, 89 & 91

[93] When considering these points, note also the provisions of sub-section 7(3)(a) of the Protection from Harassment Act 1997 and the definition given of harassment.

[94] Marti Blagborough can be seen doing this explicitly in the following content from Street Video Reviewer: *Marti Blagborough Is A Nutjob*
https://www.youtube.com/watch?v=sHI6uNYcIRc

above, victims are often left having to submit repeated complaints to YouTube about the same content and ultimately will throw in the towel and be left feeling powerless.

The legal position of YouTube in regard to “auditors” can be summarised as follows:

1. YouTube is currently not complying with its data protection obligations in regard to “auditors”.

2. It is important to understand that the ‘conditional immunity’ enjoyed by YouTube as a third-party content platform is only valid to the extent that it acts promptly on reports or discovery of “auditing” content.

3. The reality of the situation is that:

    3.1. YouTube has long had corporate knowledge of the “auditing” phenomenon, has constructive knowledge of what “auditors” do and the nature of their activities due to innumerable complaints about them, and knows or has constructive knowledge of, the problem of circumvention outlined in (iii) above.

    3.2. Despite all this, YouTube has failed to act decisively or effectively to manage and limit, or demonetise or remove, “auditing” channels from its platform.

    3.3. Thus, YouTube is not availed of ‘conditional immunity’ because the harms caused by “auditing” content have become ‘foreseeable’, and in the eyes of the law, YouTube is directly responsible and liable for the content of all “auditors”.

Relevance of all this to the police

The above information provides a background to the digital environment in which “auditors” operate. It is the view of the author that the police should be working alongside the ICO and YouTube to address and curtail the activities of “auditors”. If YouTube is unwilling to co-operate in efforts to deal with “auditing”, then as explained above, there is the potential for vicarious criminal liability for YouTube corporately and for any prosecutable corporate officers, executives and other staff - especially in circumstances where YouTube (or whatever social media platform is involved) is allowing repeated use of the same image or content, as this would potentially form the offence of criminal harassment contrary to section 2 of the Protection from Harassment Act 1997[95].

[95] See in particular the definition of harassment given in sub-section 7(3)(a) of the 1997 Act.

6. The police response to Social Media "Auditing"

The current policy position

The ACPO Communication Advisory Group Guidance 2010[96] ('2010 Guidance') was issued to inform the police approach to media generally, and the Commercial Advisory Group also issued statements from the then-chair, Andy Trotter, concerning public photography specifically ('the Trotter Guidance')[97]. It must be acknowledged that those documents pre-date the growth of social media and the emergence of the "auditing" trend during the 2010s. "Auditing" is not public photography or vlogging, and in the majority of cases, does not involve journalism or 'citizen journalism', thus generally-speaking, the 2010 Guidance and Trotter Guidance should not be applied to the activities of "auditors" as they do not cover it or in any way address the nature and purpose of what "auditors" do.

Auditors/Social Media Bloggers – Initial Guidance, v.1.4 issued by the NPCC in December 2021[98] – follows in much the same vein and lumps "auditors" in with photographers and vloggers, rather than recognising "auditors" as a discrete and separate trend that is not legal or lawful. It is also important to note that that document was published during the period when Covid-19 lockdowns were still in place and policing responses had to be guided by a very different context compared to today.

These various policies sit within the framework of three Authorised Professional Practice (APP) documents issued by the College of Policing that are of particular pertinence to "auditing":

- APP on Critical incident management (2013)[99]. This knits in with the National decision model[100] and the Joint decision model[101], which further guide officers, PCSOs, staff, partners and stakeholders on responses to incidents.

- APP on Conflict management (2024)[102].

---

[96] https://www.whatdotheyknow.com/request/guidanceposition_on_photography/response/685795/attach/5/CAG%20Guidance%202010.pdf?cookie_passthrough=1

[97] The 2010 published guidance was preceded by a published open letter ('Guidance for Photographers') to forces from the Chair of the ACPO Communication Advisory Group: https://www.theiac.org.uk/resourcesnew/filming-in-public/ACPO_Guidance_PhotographsPublicPlaces.pdf

[98] https://www.whatdotheyknow.com/request/auditors_social_media_bloggers_i/response/1721570/attach/5/AuditorsSocial%20Media%20Bloggers%20Guidelines%20v3.pdf?cookie_passthrough=1

[99] https://www.college.police.uk/app/critical-incident-management

[100] https://www.college.police.uk/app/national-decision-model/national-decision-model?s=

[101] https://www.jesip.org.uk/joint-doctrine/the-joint-decision-model-jdm/

[102] https://www.college.police.uk/guidance/conflict-management

- APP on Engagement and communication (2013)[103].

Police responses 'on the ground'

As a result of a muddled and outdated general policy position, police responses to "auditing" have been confused and characterised by inconsistency. In some disturbing cases, officers have even complied with the demands of "auditors", arresting innocent individuals on allegations such as assault[104]. There have been at least two cases where individuals have ended up with criminal records as a result of provocation from an "auditor"[105] and there are likely to be many more.

"Auditors" have been subject to sporadic action by the law – including arrest and criminal prosecution – ever since "auditing" began in this country[106]. One or two have served prison sentences for activities relating to "auditing". Most have been fined and received Criminal Behaviour Orders (CBOs)[107]. It is believed that one reason most auditors now don't visit police stations is that the police started prosecuting them for aggravated trespass and/or other related offences and, as part of sentencing, the courts granted CBOs that barred them from police premises (save for if they had proper business with the police). In consequence, word got round and "auditors" started focusing on private businesses instead.

---

[103] https://www.college.police.uk/app/engagement-and-communication

[104] For example, the disturbing case involving Marti Blagborough, who harassed a car wash and was hit with a metal bar by the irate owner. The owner was charged and prosecuted while Marti Blagborough faced no action. See this video from Marti Blagborough's YouTube channel:
I Got Hit With a Metal Bar, Punched Him Back. Thug ARRESTED
https://www.youtube.com/watch?v=LX8VecSsBcQ
Another example is an incident in which PJ Audits visited a scrap yard and was threatened by the employees, one of whom received a caution while no action was taken against PJ Audits.
Assaulted By 5 People Police Attended, Full Video
https://www.youtube.com/watch?v=tHTv_U1955Y
In the following video, DJ Audits harassed a chemical company and he was assaulted by a manager, who was then forced to write an apology by a police officer.
Libra Speciality Chemicals Ltd Assault | Update Video
https://www.youtube.com/watch?v=JbY2Q67glUo
In no way does the author seek to condone the actions of the staff involved in these incidents, but it is very concerning to note that police officers seem oblivious to the true nature of the "auditor's" actions in each case, instead simply blaming the victim of the "auditor" - perhaps with some basis in law, but nevertheless this does seem unfair and must harm public confidence in the police.

[105] Ibid

[106] Youtube vlogger admits Macclesfield police car park 'audit' trespass
https://www.bbc.co.uk/news/uk-england-manchester-59388860#:~:text=Cheshire%20Police%20said%20Lee%20Tench,admitted%20aggravated%20trespass%20in%20court.
Man convicted after he admitted to filming on his phone inside Wellingborough Magistrates' Court
https://www.northamptonchron.co.uk/news/crime/man-convicted-after-he-admitted-to-filming-on-his-phone-inside-wellingborough-magistrates-court-3260120

[107] n 8

Unfortunately, the firm action that was taken to suppress "auditing" around police premises[108] was not continued against "auditors" who visit private businesses. The author believes that police officers are working to outdated policy guidance that shoehorns auditors into the category of 'photographer', and there is perhaps also a fear on the part of individual officers about being portrayed negatively on social media, exacerbated by a lack of clear direction on the issue. This has led to a pattern of weak or confused responses, and non-responses from the police in general, which has encouraged the perception that auditors are doing nothing wrong.

Typical police responses to "auditing" incidents

Responses to "auditors" on the part of officers tend to be from either extreme, either:

- overly aggressive and overbearing, often accompanied by an inaccurate appraisal of the legal position that seems intended to suppress public photographic activity; or,

- overly friendly and conciliatory, again typically accompanied by an inaccurate understanding of the legal position that ignores the true nature of what the "auditor" is up to[109].

The first approach is a potential threat to the civil liberties of innocent photographers, whom officers may not distinguish from "auditors".

The second approach ignores the rights and concerns of the victims of "auditors".

"Auditing" as a Critical Incident: how the police should respond

The College of Policing APP on Critical incident management (2013)[110] defines a Critical Incident as:

"…as any incident where the effectiveness of the police response is likely to have a significant impact on the confidence of the victim, their family and/or the community."

---

[108] Which seems to have arisen at least in part from concerns amongst officers about their privacy. See for example:
Dealing with the WORST UK Police Auditors | Retired Police interceptor
https://www.youtube.com/watch?v=xwlLYHP2QWM&t=11s

[109] n 10 & 19

[110] n 99

"Auditors" do have some support on social media, and the largest "auditing" channels on YouTube have many thousands of subscribers[111], but they do not have the support of the wider community. They are not photographers or vloggers[112], they are not undertaking a legal activity[113]. They are in fact undertaking an activity that is harmful[114] and is broadcast on prominent social media platforms; therefore the maintenance of public confidence in the police must be a factor in how the police respond to these incidents, which should be considered to be Critical Incidents (or potentially so).

Where it appears the "auditor" intends to, or is behaving in a disorderly manner likely to, cause harassment, alarm or distress, or is committing or has committed other offences at the location (such as aggravated trespass), officers should escalate the incident.

As a first step, where the individual is not simply an ordinary photographer or vlogger, officers should be instructed to always invoke the power to take the name and address of the "auditor", pursuant to section 50 of the Police Reform Act 2002 ('section 50 information'), relying on the definition of 'anti-social behaviour' in sub-section 2(1)(a) of the Anti-social Behaviour, Crime and Policing Act 2014. The section 50 information should then be checked with force intelligence while the auditor is detained. The officer should then use his own judgement to further appraise the situation and decide on the appropriate course of action, taking into account whether it has been verified that the detainee actually is an "auditor", the seriousness of the incident, and the wishes of anyone at the scene who may wish to make a complaint. Action may include one or some combination of the following:

(i). no action and/or simple de-escalation, where it is apparent the "auditor" has done nothing wrong on this occasion or the anti-social behaviour involved is of a trivial nature;

(ii). words of advice to the "auditor" and/or the occupier (where words of advice are to be given to the occupier, this should be done out of sight of the "auditor"). Words of action for an "auditor" may be most appropriate where it is apparent the auditor has done something wrong but the occupier is reluctant to pursue a complaint about it;

(iii). anti-terrorist suspicion-based stop and search. The stop and search power in section 43 of the Terrorism Act 2000 should be used only when reasonable suspicion exists that an article relating to terrorism will be found.

---

[111] The largest purely "auditing" channel, Auditing Britain, currently has 286,000 subscribers, as at 26th. July 2024.

[112] n 45 & 46

[113] n 44 & 47 and see section 3 above.

[114] See section 3 above for a summary of the relevant law, section 4 above for a discussion of the business perspective on "auditing", and section 7 below for a summary of the harms involved.

The appropriate use of this power is therefore likely to be restricted to incidents in which the actions of the "auditor" bear similarity to what that may be expected of a terrorist (see discussion of *simulating suspicious behaviour* and *simulated hostile reconnaissance* in section 2 above (pp. 17-18);[115]

(iv). diversion. This may be an appropriate outcome in combination with one or more of the other outcomes where the "auditor" has obvious social vulnerabilities or manifestly has severe mental health issues. Officers may refer the "auditor" to Liaison and Diversion (L&D) services within the local NHS. Consideration should also be given in these circumstances to using powers under section 136 of the Mental Health Act 1983 if it is felt that the individual is suffering from acute mental ill-health and in immediate need of care and control. It is suggested to seek the advice of a clinician in advance to ascertain if the individual is known to local mental health services and receiving care or treatment.

(v). dispersal. "Auditors" typically operate by visiting a number of public buildings or businesses in the same vicinity. Section 34 of the Anti-social Behaviour, Crime and Policing Act 2014 gives dispersal powers for officers in a locality on the authorisation of an inspector[116]. This power could be used where it is reported that an "auditor" is operating in a given area. On invocation of the power, officers would be able to attend at the scene and require that the "auditor" should disperse. Where applicable, this may be the appropriate outcome in conjunction with one or more other outcomes listed here;

(vi). issuance of a Community Protection Notice on the "auditor". This could be appropriate where the 'section 50 information' reveals that the "auditor" lives locally;

(vii). a report for summons of the "auditor". This could be appropriate where the occupier has confirmed they wish to pursue a complaint and it is likely that sufficient evidence is available without having to seize the "auditor's" own photographic equipment;

(viii). an arrest for the purpose of preserving evidence under the general power in section 23 of the Police and Criminal Evidence Act 1984.

Officers should be required to also carry out further intelligence tasks following such incidents, including:

---

[115] It is unlikely a routine suspicion-based stop and search under section 1 of the Police and Criminal Evidence Act will be appropriate or a relevant power to use with very many "auditors", given the type of offences involved.

[116] This must be for the purpose of removing or reducing the likelihood of behaviour occurring that is likely to cause harassment, alarm or distress – see sub-section 34(2)(a) of the Anti-social Behaviour, Crime and Policing Act 2014.

- an entry on the Police National Computer (PNC) in regard to the suspected individual;

- entry of the 'section 50 information'[117] on a force intelligence file;

- ideally there should also be ability for officers to enter 'section 50 information'[118] on a central intelligence repository held by Scotland Yard, the National Crime Agency (NCA) or the NPCC for this purpose that will allow forces to raise enquiries nationally about individuals and share information.

Where a prosecution is pursued, the Crown Prosecution Service (CPS) should be instructed at an early stage to pursue a Criminal Behaviour Order (CBO).

Police officers should avoid:

- a debate with "auditors" about photography laws or the legitimacy of police action against "auditors" in the specific situation at hand or in general;

- (except where it appears the "auditor" has a bone fide criminal complaint against the occupier or member of staff) any action that appears to appease or side with the "auditor", such as giving words of advice to the occupier in front of the "auditor". What is most offensive about this is that the occupier can then be portrayed by the auditor as in the wrong for not understanding public photography rights – which is a debatable point in the circumstances anyway, as what auditors do is not photography/vlogging in the first place, it is instead clearly intended to provoke and annoy businesses and workers[119];

- over-friendliness in an effort to get on side with "auditors" and not be portrayed badly on social media[120]. Officers should always be civil and polite with "auditors" (use of the salutation 'sir' or 'Mister', etc'), but the duty of a police officer is to enforce the law and keep the peace. "Auditing" is not a legal activity, thus there is no obligation on police officers to maintain good public relations with "auditors"[121], which

---

[117] Information obtained pursuant to section 50 of the Police Reform Act 2002.
[118] Ibid
[119] For an example, see this video from BP Visits:
It's Private Property So You Shouldn't Be Going Above! - Police Attend! - Part 2
https://www.youtube.com/watch?v=2cZCvKV6S7g
[120] n 10
[121] For a more assertive defence of officers, see this pubic statement and presentation by a sheriff in the United States following a vexatious complaint by an "auditor":
1st Amendment Auditor Issues Apology
https://www.youtube.com/watch?v=mO4NDs7MGpk

"auditor" will just take as a sign of weakness. If individual police officers have concerns about their own privacy, forces should support them fully in complaints to YouTube.

Political and public relations implications

In reality, "auditing" is a marginal trend and not widely popular amongst the public. The attached "List of Social Media "Auditors" in Appendix III to this paper shows that even the most popular "auditing" YouTube channels maintain less than 500,000 subscribers currently, despite many years of effort and consistent content, and the vast majority of monetised channels have less than 20,000 subscribers. If a force has concerns about public perceptions of officers' actions in a particular incident, it can issue clarifying statements on its website and social media that emphasise some of the points made in this paper – especially the fundamental distinction between genuine public photography and vlogging on the one hand[122], of which there are millions of YouTube channels that upload content daily without issues with the law, and "auditing" on the other hand, which is not a legal activity[123].

Now compare this to the apology given to Auditing Britain by an officer of Professional Standards Department of West Mercia Police:
https://www.youtube.com/watch?v=TzGVogTAGLM
This apology was not necessary, as Auditing Britain is not a vlogger or photographer. He is a police baiter. With respect, this makes the police look weak.

[122] n 45 & 46

[123] n 44 & 47 and section 3 above

7. Civic, social and personal harms of Social Media "Auditing"

7.1. Civic harms

The problem of police officers, security staff and random members of the public objecting to public photography – often on the basis of fundamental misunderstandings of the law, has always existed for photographers – probably for as long as cameras have existed, and it will always exist for as long as photography exists. No matter how well educated people are about public photography rights, there will always be some objections to it in day to day reality because some people don't like to be photographed and may even feel violated by it. In the absence of an overriding justification, this should be respected. The law may not always require photographers to respect people's qualms, but good manners does demand it - in most cases. Most street photographers (including the author) take it in their stride with no big problems or dramas.

The concern about "auditing" is "auditors" do not have the balanced mindset of normal people and their obnoxious activities are having a 'poisoning the well' effect[124] and making things worse for genuine photographers and vloggers. Some people (on both sides of the debate) have a narcissistic frame of mind and enjoy being the 'star' of their own little drama.

In the context of "auditing" specifically, as discussed above (page 26), some staff may approach "auditors" on purpose in the knowledge they are being filmed, seeing some appeal in the prospect, and intent on starting an argument or confrontation with the "auditor" (perhaps in disapproval of what they do). In the case of "auditors", they make a big song and dance over what they perceive to be their own rights. This over-emphasis fails to appreciate that individual rights, while very important, do not exist in a vacuum, and must be balanced with the rights and dignity of others in a way that is consistent with a liberal-democratic society; once this is forgotten, those rights could be under threat by those who seek to impose formal restrictions on the basis that photographers (in fact, "auditors") cannot regulate their own behaviour.

"Auditors" argue that they are contributing to a more open society, but the right to photograph in public does not extend to causing harassment, alarm or distress for others or infringing on the rights and liberties of others in the various other ways that "auditors" do. Photography and vlogging do have an important role in public scrutiny – as well as art and culture – but at root it should be a pleasant, harmless vocation or avocation, not associated in people's minds with bullying and mobbing and other unpleasant behaviour. Once photography is associated with those things, the rights and liberties of photographers could be brought into question, a situation that could ultimately

[124] https://en.wikipedia.org/wiki/Poisoning_the_well

harm the cause that “auditors” claim to fight for, with devastating impacts on democratic engagement in society.

7.2. Social harms

The manner in which “auditors” present the police lowers public confidence in the police and the activities of “auditors” against both the police and businesses, and public bodies generally, corrodes social trust and undermines the normal exercise of civil liberties.

Under the guise of content creation, “auditors” are using public spaces as stages for harassment and invasion of privacy. In this way, the most devastating impact of “auditing” on wider society is on the atmosphere in society. “Auditors” help to poison social media by commercialising hate. When individuals and businesses rightfully defend themselves, or question and challenge “auditors”, they become targets of hateful and dismissive comments online and harassment. These attitudes then bleed into wider society.

“Auditors” and their online supporters often display misogynist and hateful attitudes towards women – including frequent use of the word ‘Karen’ as a dismissive epithet, both verbally during an “auditing” visit and also in the video titles and descriptions and in comments beneath videos[125]. It is true that use of the slang meme word ‘Karen’ is widespread on social media and can often be interpreted as nothing more than good-natured jocularity, but “auditors” (and their supporters in comments online) habitually label any women they

[125] Numerous examples can be found. See these links:
https://www.youtube.com/watch?v=pkzeb5Ygs3M&t=630s
https://www.youtube.com/watch?v=fslupZcI1pc&t=264s
https://www.youtube.com/watch?v=AtKJzN9GUFU
https://www.youtube.com/watch?v=nbq2f429NBs&t=593s
https://www.youtube.com/watch?v=3NutV_LJnzM&t=368s
https://www.youtube.com/watch?v=vxb5mhTRR7k
https://www.youtube.com/watch?v=109q3Jpnh9Y&t=35s
https://www.youtube.com/watch?v=l2dBd9MG2AY&t=121s
https://www.youtube.com/watch?v=9vp4ncaxKHI
https://www.youtube.com/watch?v=yfIdUar3zvI
https://www.youtube.com/watch?v=QkBMmEPDe9Y
https://www.youtube.com/watch?v=kynp-BfbXWg
https://www.youtube.com/watch?v=1CtBXfcMHCU
https://www.youtube.com/shorts/RhE9RRYYN-k
https://www.youtube.com/watch?v=plYPiHMSxFk
https://www.youtube.com/watch?v=7MI7VZqifwk&t=46s
https://www.youtube.com/watch?v=kW8e8Xe70ms
https://www.youtube.com/watch?v=z-OV0HB5RZc&t=521s
https://www.youtube.com/watch?v=MTRpDcknUxQ&t=80s
https://www.youtube.com/watch?v=YQtJFJoomCI

encounter this way and use it bully them and to dismiss their concerns about the activity.

7.3. Personal harms

"Auditors" brazenly film unsuspecting individuals and proceed to mock and verbally insult them, targeting people of all demographics—old, young, women, and men—in a calculated attempt to provoke reactions and elicit anger. When someone naturally reacts to this harassment and attempts to defend themselves, the "auditor" will often insult and belittle the victim(s) further. This is all part of the "auditor's" scheme to generate scandalous content for their YouTube channel, garnering clicks, likes, and hate comments at the expense of innocent people's reputations and well-being. It is a sinister ploy, commercialising their activities by tarnishing the public image of others.

"Auditing" is, in short, based on the abuse of others and exploits the average person's normal and natural reaction to being intrusively filmed, and exploits the fact that the majority of ordinary people will not have a grasp of the finer points of public photography law (not that any "auditors" have much of any grasp of the law either). Victims who know they have been filmed have to wait until footage is uploaded to social media, and often don't know where it will be uploaded, which must cause great anxiety for many. Some people lose their jobs after the footage has been uploaded, merely because they are perceived to have been rude to the "auditor" or carried out their duties in a way that their employer did not like. Victims are made to look foolish in edited footage uploaded to social media, which adds to their distress and may cause or exacerbate mental health issues.

A sub-trend amongst "auditors" has been to attend and film at job centres. Claimants attending job centres often feel vulnerable because claiming benefits involves having to discuss one's personal circumstances. If a strange man (often masked) is walking round the public area filming people's faces (which are not then blurred in the uploaded footage), this is likely to cause distress to claimants and service users[126].

[126] Playlist from Street Video Reviewer covering "auditors" filming in job centres: https://www.youtube.com/watch?v=YWDmFc1C1pg&list=PLVNCkW0EZUy6vjeSWlu7asqE63PTQOQDX

8. The need for a strategic approach

A ‘strategic approach’ simply means an approach to the problem that is co-ordinated and planned and results in a consistent application of the law. Due to its nature, a strategic approach should also embrace working in partnership and co-operation with other agencies, organisations and private sector providers. This could include partnerships and co-operation centrally and also at the intermediate level on the part of individual forces with local partners (as discussed in section 9 of Appendix IV of this paper).

What characterises the police response to “auditing” so far is the opposite: it has been in silos, with officers from the various forces responding to each incident in isolation with muddled, confused and inconsistent application of the law from one incident to another, with some officers being overly-friendly and appeasing towards “auditors”, while others are overbearing – all of this reflecting the lack of the coherent understanding of what “auditing” is and involves that could inform a strategic approach to the problem.

One practical consequence of the lack of a strategic approach is seen in how officers who respond to these incidents often seem either unaware that the individual is an “auditor”, or if they are aware of this, they treat the “auditor” as just another photographer or vlogger, and even proceed to berate staff who the “auditor” has just been victimising on camera.

As a first step, the police should develop a policy on social media “auditors” that provides a quite separate treatment to that afforded to public photography. A draft policy is provided in Appendix IV of this paper.

The police should also try to build links with the ICO and YouTube in order to co-ordinate efforts and work together to tackle the problem. These efforts could be part of wider initiatives to address harmful social media or could be specific to “auditing”.

In a recent letter to the ICO (found in Appendix II of this paper), the author has set out some outline recommendations for partnership working between the ICO and YouTube, and the police could also consider contributing to this by providing liaison for YouTube, the ICO and victims of “auditors” to raise concerns and report the specific activities of “auditors”.

9. Laws and powers that response officers can make use of 'on the ground' to disrupt, deter and discourage "auditors"

Powers are available to police officers to deal with "auditors" and to ensure the application and enforcement of the relevant law as discussed in section 3 above (pages 21-23):

- The most fundamental power of any constable is the ancient common law power to arrest a person for a breach of the peace or for conduct that threatens or is likely to result in a breach of the peace. A breach of the peace is not in itself a criminal offence, but the power of arrest and de-arrest would serve as an effective method for officers to de-escalate incidents and disrupt and deter the activities of "auditors".

- Officers have the power under section 50 of the Police Reform Act 2002 to demand the name and address of any person the officer believes is behaving in an anti-social manner. This power ought to form the basis of police intelligence collection against "auditors". The information obtained under section 50 can be cross-checked with intelligence held by the force or nationally on "auditors" and if it is found that the individual is an "auditor", this could inform further escalation of the incident, including reporting for summons or arrest, because it would serve to clarify the troublesome individual's purpose and intentions, that the troublesome individual's behaviour in the situation at hand is unlawful and anti-social, and specifically intended to, or likely to, cause harassment, alarm or distress, etc.

- Officers can make use of the stop and produce powers under sections 163 and 164 of the Road Traffic Act 1988.

- Article 13 of the UK GDPR requires that a data controller identify him/herself to a data subject. There is no express power to immediately enforce this in any given situation, but officers should be made aware of Article 13 because any refusal to comply could be reported by the force to the ICO and YouTube respectively, and if repeat complaints are received about the same person/content creator, either or both may then take action. The ICO in particular has the power to fine individuals for breaches of data protection and may elect to do so where it is apparent that the breaches are numerous and systematic – as they always will be on the part of an "auditor".

- "Auditors" typically operate by visiting a number of public buildings or businesses in the same vicinity. Section 34 of the Anti-social Behaviour, Crime and Policing Act 2014 gives dispersal powers for officers in a

locality on the authorisation of an inspector[127]. This power could be used where it is reported that an "auditor" is operating in a given area. On invocation of the power, officers would be able to attend at the scene and require that the "auditor" should disperse on the grounds that he is engaging in behaviour likely to cause harassment, alarm or distress[128].

- Constables and PCSOs (if so designated) are empowered under section 43 of the Anti-social Behaviour, Crime and Policing Act 2014 to issue Community Protection Notices, which could be a useful and effective way of disrupting the activities of an "auditor" where he is operating in his own locality.

[127] This must be for the purpose of removing or reducing the likelihood of behaviour occurring that is likely to cause harassment, alarm or distress – see sub-section 34(2)(a) of the Anti-social Behaviour, Crime and Policing Act 2014.

[128] Section 35(2) of the Anti-social Behaviour, Crime and Policing Act 2014.

10. Addressing common objections to enforcement against "auditors"

Photography is not a crime/It's just photography, etc.

That's as silly as saying that an armed robber is not committing a crime if he films himself robbing a bank, or somebody who commits upskirting should not be criminally prosecuted because he was using a camera. The slogan, "Photography Is Not A Crime", does not represent a complete statement of the law. It would be more accurate to say that the default position throughout the UK is that photography is legal except in specific situations and circumstances restricted by law, and people who use a camera or other recording device to commit offences or civil wrongs are not excused from the consequences of their actions in civil or criminal law.

"Auditing" is legal

This is a subtle variant on the previous argument. If "auditing" is legal, then behaviour involving or likely to cause harassment, alarm or distress, common assault, and aggravated trespass must all be legal, and civil wrongs such as simple trespass, as well as the whole body of data protection law, should be ignored. Clearly this is not a tenable position. The refrain 'auditing is legal' is really just a way of saying that we shouldn't bother too much about it – which is a matter of opinion only.

"Auditors" have improved official understanding of public photography rights

This is not true. There were public photography and vlogging channels on YouTube before "auditing" became a social media trend and there are millions of such channels today that report few or no issues with the exercise of their public photography rights. Where they do report issues, this usually takes the form of simple objections on the grounds of manners or privacy in the context of genuine photography or vlogging, and the content creator can resolve the issue or take it in his stride. There is no need to turn petty disagreement of this sort into histrionic drama.

Even if it were true that "auditors" have contributed to greater tolerance towards photographers and their rights, the same result could have been achieved without "auditing". At best – and this is to be extremely generous – "auditing" has proved to be a necessary evil, and the necessary evil argument is always a bad justification on closer examination because any benefits come at the expense of costs that often outweigh the benefits. In the case of "auditing", the potential costs are the erosion of goodwill towards photographers, vloggers and drone operators due to the irresponsible actions of "auditors"; the harms inflicted on the victims of "auditors", which will be largely psychological and difficult to quantify, but will also include losses and

damages to businesses harassed and victimised by “auditors and their followers; and, the erosion of trust and confidence in the police amongst the public, due to the misleading portrayal of police actions by “auditors” and others who support them.

It’s citizen journalism

“Auditors” are not journalists and very little of their content could be considered journalistic in nature. The behaviour of “auditors” is far removed from what would be reasonably expected from even the most aggressive citizen journalist or investigative vlogger.

People should just ignore them, then they’ll go away

For the reasons explained above in section 4 (pages 24-26), ignoring “auditors” may work in specific situations, and does form part of the solution to it, but it is not a viable tactic generally. Workplaces and public buildings are concerned with security and it is common workplace culture in the UK that all staff should look out for strange people hanging around, near or on premises. Strange people have to be challenged or reported or both. To demand otherwise is to propose that workplaces should stop being concerned about the security of their staff, customers and clients, visitors, buildings, and other assets. It is not realistic. “Auditors” know this, which is why “auditing” channels still exist after all this time. In essence, what “auditors” are doing is exploiting the normal and natural reactions of staff and security to their presence – it is a crude type of social engineering. A more effective and intelligent solution is needed to the problem than just lazily telling people to “ignore” it (even if, admittedly, that advice can work and may form part of the solution).

It’s just a camera, get over it

It is not just a camera. If it were, there would be no problem and no need for this paper or any complaints.

When police officers/security/staff are nice, nothing happens

This objection is objectionable for two reasons. First, it is not the duty of police officers or people in general to be ‘nice’ to “auditors” or anyone else. The demand that they should be is bossy and authoritative and amounts to further abusive and disdain towards working people. It reflects the childishness and immaturity of “auditors” and their overbearing need to impose their wishes and beliefs on everybody else. Besides all that, niceness does not necessarily equate to professionalism or dutifulness.

The general duty of police officers is summarised in the oath of attestation[129] that can be distilled as a duty to police without fear or favour. Police officers are expected to be civil (not the same as 'nice'), to be polite where possible (again, not the same as 'nice'), and to be a friend to the law-abiding (which does not entail being 'nice' to "auditors"). Police officers who prioritise being 'nice' and pally and addressing members of the public as 'mate' become pliable[130]. Similar can be said for security staff and workers that "auditors" encounter, all of whom have duties to their employers, which may include challenging strange men who turn up at premises wearing masks and filming.

The victims are rude and abrasive and bring it on themselves

It is true that some of the victims of auditors are lacking in social skills or professionalism and bring embarrassment on themselves by being rude and abrasive, but that does not mean these people deserve it and in no way does it justify what "auditors" do. They are only a small minority of victims anyway. Most of the victims are blameless, innocent working people simply going about their lives.

What about the fact that some people consent to being in/are evidently happy to be in "auditing" footage?

Not the point. Many of those people will have no idea that their facial image will be uploaded to social media or may not fully appreciate how this potentially compromises their privacy – in other words, they are not giving informed consent. The "auditor" will not help them understand all this, that is for certain.

You're making too much of it. A lot of the people captured in "auditing" content don't mind

Some don't mind the attention and don't care if their faces appear on social media, but that is not the point. "Auditors" usually pose as "members of the public" and rarely disclose what the purpose of filming is or where the footage will appear, or the fact that it will be broadcast at all. Often when people are nice to "auditors", it is partly because they are oblivious of the trend and unaware that the footage will be broadcast on social media and simply assume the "auditor" is just an inquisitive visitor. In some cases, the "auditor" is filming covertly.

"Auditing" is harmless

Harassment, alarm or distress, simple trespass, aggravated trespass, breaches of privacy and data protection, etc., etc., are not harmless.

---

[129] See Schedule 4 of the Police Act 1996 (as amended).

[130] n 10

The trend will go away on its own. Eventually businesses will wise up to these "auditors" and viewers will get bored of it and a new craze will take its place

We can't rely on that, and this objection goes to the core of the problem. If "auditing" is not tackled now when it is still a relatively marginal trend, the risk is that it could develop out of control and members of the public and staff at premises may start to take the law into their own hands (there have already been incidences of this). The danger at that point will be that elected politicians may start to demand further restrictions on public photography rights, meaning that everyone's civil liberties will be undermined due to the actions of a tiny few.

"Auditing" is a small trend in the grand scheme of things. You're proposing a sledgehammer to crack a nut

Nobody pretends that "auditing" is a serious matter in criminal terms, however "auditing" is not photography/vlogging or journalism, and while it is not serious in nature, virtually any kind of low-level offending that is nonetheless harmful could be vulnerable to the argument that the authorities shouldn't bother. It is highly disingenuous to dismiss complaints and wider concerns on the basis that "auditing" doesn't seem serious when, in reality, it is an organised activity that is plainly different to photography and journalism and clearly intended to cause annoyance and distress for the enrichment of "auditors". Ultimately, the police exist to serve the public, not the other way round, and the argument that something is too trivial to bother with seeks to deflect from acknowledging this.

"Auditing" is a harmful activity that often involves the commission of civil wrongs and actions that are contrary to the criminal law. The police have a duty to uphold the law and keep the peace and - subject to the exercise of police discretion[131] - cannot pick and choose which laws to enforce based on personal preferences or a vague belief that something 'isn't all that serious'.

We don't have the laws/powers that can stop them. We need new laws

We don't need new laws. As explained in sections 3 and 8 above, existing laws and powers are more than adequate to deal with "auditors". The police and courts have already used their powers to deter "auditors" from attending

---

[131] "*Police officers must be allowed to police with discretion. Discretion is the bedrock of policing; it allows reasoned and fair decisions based on experience to be taken by police officers without the need to take a course of action merely to satisfy targets.*" Page 4 of *The Office of Constable - The bedrock of modern day British policing*, published by The Police Federation of England and Wales. https://www.polfed.org/media/14239/the-office-of-constable-with-links-2018.pdf

police stations and most of them now stay away from police premises. This was a highly effective use of existing laws and powers to deal with the trend, involving the imposition of Criminal Behaviour Orders against select “auditors”. Once word got round, most “auditors” stopped bothering the police or became much more careful in how they went about it.

The same approach is now needed to protect the country’s workers and businesses from these people, and the police and the courts have ample powers at their disposal to deal with the problem. There is no need for new laws or any change in the law. What is needed is a change in policy in which the police at a national level develop a distinct approach to the problem so as to minimise its harms, and seek to work in strategic partnership with others, including the ICO and YouTube, to stop it for good.

You don’t understand the internet. If you ban people, they will just pop up elsewhere

Even on its own terms, this objection is not true because YouTube is perfectly willing and capable of banning channels and users from its platform and does so daily. YouTube has in the past terminated channels on the basis that they are part of a harmful trend – for example, between 2015 and 2020, scores of large and prominent channels were terminated and/or demonetised by YouTube because of their association with the political far-Right. While “auditors” do upload their content to a variety of platforms, they are reliant on YouTube for the majority of their income and kudos.

This paper does not propose that anyone should be banned from the internet altogether. What is proposed, amongst other things, is that effective use is made of existing laws and powers to minimise, deter, disrupt and stop the activity for good. This may involve the imposition of controls on the photographic and internet activities of individual “auditors” through Criminal Behaviour Orders. For instance, an auditor could be banned for a set period from filming private premises (whether or not from a public right of way) without the consent of the occupier, and could also be banned from setting up, running or having any involvement in a YouTube channel.

11. Conclusions

Social media “auditing” is an unlawful and anti-social activity that causes harm to innocent people, not a type of public photography or vlogging.

Police policymakers should review and change police policies on public photography/vlogging so that a clear distinction is made between public photography/vlogging on the one hand and social media “auditing” on the other, and officers and others should be encouraged to pursue the appropriate response to the activity, wherever it takes place.

A change in policy may assist response officers, PCSOs, police staff and others to deal effectively with incidents involving social media “auditors”, both on police premises and on commercial and public premises where officers are called to attend. It is hoped a shift in policy may contribute to discouraging and deterring the activity.

In conclusion, the author calls on the National Police Chiefs’ Council and the various police forces to agree and promulgate a national policy on social media “auditing” - emphasising its separateness from public photography and vlogging - to assist officers and others by identifying the relevant criminal offences involved in the activity and guidelines to follow in encounters with “auditors”.

APPENDICES:

I. “Auditing” methods and blueprints

II. Copy of letter to the ICO, dated 15th. May 2024

III. A list of social media “auditors” as at July 2024

IV. Proposed draft Model Force Policy On Social Media “Auditors”

APPENDIX I:
"Auditing" methods and blueprints

Here are summaries of the typical approaches and tactics of some of the more prominent "auditors":

1. Auditing Britain[132]

Auditing Britain, aka Reda Bouadi-Clifton, is a mini-cab driver based in Banbury, Oxfordshire. He uses a variety of tactics from one video to the next, but one of his most favoured tactics is to bait the police by simulating hostile reconnaissance. This is when he walks round a police station filming in building windows and through the windows of cars. Inevitably this attracts the attention of officers who then challenge him, and he films the encounter and edits the footage in such a way as to make it look like he is being harassed as an innocent photographer and perhaps being racially profiled (one factor that aids the simulated hostile reconnaissance tactic is that he is of northern African descent).

It is the author's view that simulated hostile reconnaissance is an offence of obstructing a police officer, contrary to section 89 of the Police Act 1996[133]. It is also possible that this behaviour is also caught by the public order offences in sections 4A and 5 of the Public Order Act 1986.

Invariably, the tactic involves trespass and an aggravated trespass is being committed in some of these incidents, as well as potentially the offence of unlawful obtaining of personal data contrary to section 170 of the Data Protection Act 2018.

Another tactic he frequently uses is what the author calls 'decontextualisation', which takes the form of commenting on, and even interfering in, stop and searches as they happen nearby, while vocally provoking and taunting the officers in attendance and portraying the officers as abusing their powers[134].

This is in addition to numerous breaches of data protection that he routinely commits on his visits. He is also not registered as a data controller, as required by Regulation 2 of the Data Protection (Charges and Information) Regulations 2018, for which he could be fined by the ICO.

---

[132] https://www.youtube.com/@AuditingBritain
[133] n 71
[134] n 61

2. DJ Audits[135]

DJ Audits, aka Nigel Dicks, is a business owner based in Leicester. He always wears a mask on "auditing" visits. His consistent tactic is to turn up at commercial premises – typically in business parks, mainly offices and warehouses - and film the buildings, staff, customers and people coming and going while standing outside. He will usually wait to be approached by security or another staff member and will film the encounter. If he is ignored, he will attempt to make contact with a member of staff. He will then inform them that he intends to fly a surveillance drone over the premises while filming any reaction this receives. He then flies the drone over site. If any objections are raised to filming or to the drone, he always dismisses or ignores these and flies the drone anyway.

Dicks can be aggressive, controlling, threatening and violent when challenged by staff or security. There has been at least two incidents when he assaulted a security guard outside a business[136].

Dicks sometimes encourages his viewers to leave malicious reviews for businesses where he has been challenged or received a negative reaction.

His tactics involve public order offences in sections 4A and 5 of the Public Order Act 1986, harassment contrary to section 2 of the Protection from Harassment Act 1997 (for instance, encouraging his viewers to leave malicious reviews), and occasionally assault. Occasionally he also commits trespass and aggravated trespass (though much less now than he used to).

This is in addition to numerous breaches of data protection that he routinely commits on his visits. He is also not registered as a data controller, as required by Regulation 2 of the Data Protection (Charges and Information) Regulations 2018, for which he could be fined by the ICO.

On one occasion, Dicks knocked down a child in Leicester while chasing a fire engine in his car. He was streaming this "audit" while it happened and the recording was leaked. It is suspected that he was not entirely truthful with Leicestershire Police about what occurred and why and instead presented the incident to the police as a simple traffic accident in which the child (on a push bike) had emerged into the junction from a red light[137].

---

[135] https://www.youtube.com/@DJAUDITS

[136] n 14

[137] See this content from Street Video Reviewer:
DJ Audits Runs Over A Child While Auditing
https://rumble.com/v3ostud-dj-audits-runs-over-a-child-while-auditing.html

3. Marti Blagborough[138]

Marti Blagborough is an "auditor" based in Leeds. He is perhaps the most unpleasant and obnoxious "auditor" in the UK, and is known to West Yorkshire Police. His tactics involve kinetic confrontation with the businesses and police officers he victimises. There have been incidents in which he has stood outside police stations shouting insults at officers. He has no compunction about committing trespass and aggravated trespass. If he is challenged by an occupier, he invariably becomes abusive and shouts at his victim(s). This "auditor" has personally harassed the author in response to the author's criticisms of him. His criminal offences and civil wrongs are numerous and cover virtually the full spectrum of those listed in section 3 above.

This is in addition to numerous breaches of data protection that he routinely commits on his visits. He is also not registered as a data controller, as required by Regulation 2 of the Data Protection (Charges and Information) Regulations 2018, for which he could be fined by the ICO.

4. BP Visits[139]

This "auditor" is believed to be from the East Riding of Yorkshire. His identity is not known at this point in time. He visits business and industrial parks in the East Riding and northern Lincolnshire and always wears a mask[140]. His tactics are identical to DJ Audits (see above) but with one or two idiosyncratic touches – for instance, he likes to 'score' the business he visits, as if to ape a genuine audit of some sort. Many of his visits are straight-forwardly public order offences under sections 4A and 5 of the Public Order Act 1986 in that he is masked, continuously filming without reason, and clearly intent on exploiting the reaction of the people he films, who are plainly often alarmed at his presence.

This is in addition to numerous breaches of data protection that he routinely commits on his visits. He is also not registered as a data controller, as required by Regulation 2 of the Data Protection (Charges and Information) Regulations 2018, for which he could be fined by the ICO.

5. PJ Audits[141]

PJ Audits, aka Peter Allsop, is a retired driving instructor based in Nottinghamshire. His "auditing" tactic is the same as DJ Audits and BP Visits described above, except on two points: first, he does not wear a mask nor attempts to conceal his identity from anybody; second, unlike the other two,

---

[138] https://www.youtube.com/@MartiBlagborough
[139] https://www.youtube.com/@bpvisits
[140] n 48
[141] https://www.youtube.com/@PJAudits

his focus is almost-exclusively on building sites and industrial sites. Unlike most of the other “auditors”, it would probably be difficult to argue that Allsop’s activities involve acts contrary to the criminal law, with the possible exception that, in common with all “auditors”, he is potentially harassing individuals by filming them without their consent in antagonistic circumstances and then uploading the result to YouTube[142]. The issues involving Allsop are mostly to do with civil law and data protection issues.

As with the others, his breaches of data protection are numerous and routine. He is also not registered as a data controller, as required by Regulation 2 of the Data Protection (Charges and Information) Regulations 2018, for which he could be fined by the ICO.

[142] Two separate ‘occasions’ as defined in sub-section 7(3)(a) of the Protection from Harassment Act 1997, forming the section 2 offence.

APPENDIX II:
Copy of letter to the ICO, dated 15th. May 2024

[Attached with the submission as a separate PDF]

APPENDIX III:
A list of social media "auditors" as at July 2024

[Attached with the submission as a separate PDF]

APPENDIX IV:
Proposed draft Model Force Policy on Social Media "Auditors"

SOCIAL MEDIA "AUDITORS"
Policy and Guidance for Officers, PCSOs & Police Staff

This Policy and Guidance supersedes and replaces the Auditors/Social Media Bloggers – Initial Guidance, v.1.4[143], issued by the NPCC in December 2021 and reflects further consultation, developments and updates to our organisational knowledge of the social media "auditing" trend.

1. INTRODUCTION

Who are Social Media "Auditors" and what is "auditing"?

1.1. Social Media "Auditors" are content creators (primarily on YouTube) who attend business premises, industrial sites, police stations and other public buildings (courts, job centres, town halls, Ministry of Defence sites, etc.), or at incidents, with the purpose of capturing workers, security staff, police officers, etc. on camera and either live-streaming or uploading the edited footage to social media platforms (typically YouTube).

What is the purpose of this activity?

1.2. "Auditors" claim that their activity is in defence of public photography rights, but "auditing" is for the purpose of earning income for the "auditor". "Auditors" do this by creating content that will entertain their viewers. They exploit security concerns of businesses and public bodies by deliberately turning up at premises to film in a conspicuous manner and by engaging in other attention-seeking behaviour. By doing so, they provoke staff and site security into reacting to their presence and challenging them, and then often proceed to assert that staff are overstepping legal boundaries, while they record the encounter for their viewers.

Are Social Media "Auditors" knowledgeable in the law?

1.3. "Auditors" tend to have a poor or incomplete grasp of the relevant law, but strongly believe themselves to be knowledgeable. "Auditors" believe they have the right to film anything in public without restriction.

---

143 https://www.whatdotheyknow.com/request/auditors_social_media_bloggers_i/response/1721570/attach/5/AuditorsSocial%20Media%20Bloggers%20Guidelines%20v3.pdf?cookie_passthrough=1

"Auditors" will often trespass on premises but deny they are trespassing and even delay or refuse to leave (claiming, for instance, that if premises are publicly accessible, then it cannot be trespass).

What does the law actually say about public photography?

1.4. There is a common law liberty in England & Wales to photograph anything one can see on or from a public right of way, subject to certain restrictions that the law imposes. Articles 10 and 11 of Schedule 1 to the Human Rights Act 1998 also support public photography rights, but again, these rights are subject to law. Photography is subject to the general law of land, including (amongst other things) criminal laws against such things as aggravated trespass and conduct intended to cause or likely to cause harassment, alarm or distress, and civil torts such as trespass to land.

Are Social Media "Auditors" the same as photographers/vloggers or citizen journalists?

1.5. "Auditors" should not be confused with photographers and vloggers. Photography and vlogging are legal activities and there are millions of public photography and vlogging channels on social media that carry out those activities without encountering any trouble with the law.

1.6. "Auditing", by contrast, is generally not a legal activity. "Auditors" are seeking to generate monetisable content through confrontation with people they encounter, such as workers, security staff and police officers, etc. Their purpose is not photography or vlogging and typically they do not produce content that could be considered journalism. They will act in an intimidating and confrontational manner, will often wear masks; they do not respect the privacy of others and do not comply with data protection laws and regulations; they will often commit civil wrongs such as trespass and commit acts that are contrary to the criminal law, such as aggravated trespass, public order offences, and common assault.

What tactics do Social Media "Auditors" use?

1.7. Typical tactics relied on by "auditors" include:

- **Conspicuously filming premises, staff, customers/clients, and other visitors**, so as to provoke a challenge from staff, an encounter that can then be filmed.

- **Provoking staff**, by attending reception, or shouting insults or taunts at staff, or trespassing, or telling staff that a drone will be flown over

site, and other behaviours intended to provoke a response that will entertain viewers (the initial provocation on the part of the "auditor" is, of course, edited out of the uploaded video).

- **Posing** as a "member of the public" or innocent photographer or vlogger, or as an "inspector" of some description, while not revealing the true purpose of the visit or that the footage will be uploaded to social media later.

- **A mass "audit", really a form of mobbing**, in which multiple "auditors" attend at premises together, with the intention of haranguing that business or public body in numbers and adding to the sense of intimidation for the people on the receiving end.

- **Covert filming**, in which the "auditor" does not disclose to staff that he is still filming or filming at all. The "auditor" may be conspicuous about filming at first, then affect to stop filming while another camera remains switched on and records what is happening.

- **Harassment**, which can take two forms. "Auditing" is inherently a form of criminal harassment in that the activity involves both the visit itself and then uploading of the footage to social media (typically the same footage is uploaded to multiple platforms and often more than once). "Auditors" may also co-ordinate multiple visits to the same premises. This is especially common if there is an adverse reaction to an "auditor". If this happens, other "auditors" will then visit those premises as a 'show of support' for the previous "auditor". There have also been occasions when "auditors" have paid repeat visits to premises in order to target particular individuals whom they perceive wronged them on a previous visit.

- **Doxxing**, is in effect a common feature of all "audits" uploaded to YouTube, since "auditors" never blur out faces. "Auditors" also seek to dox their critics online as a form of intimidation and to discourage determined criticism of their activities.

- **Simulating suspicious activity**, in which the "auditor" will act in such a way as could be interpreted to be suspicious (for example, by filming inside police cars at a police station or filming CCTV and other security features, etc.), so as to attract the attention of security staff or officers and provoke a reaction.

- **Simulated hostile reconnaissance**, similar to the above, in which the "auditor" will act in a similar way to what may be expected of a terrorist conducting hostile reconnaissance. The "auditor" may

exploit personal attributes, such as his own racial or ethnic background, in the belief that this will provoke a police response.

1.8. "Auditors" manipulate the normal and natural responses of ordinary workers. They know that the culture in most UK workplaces of any size is that staff are expected to challenge or report strange people on or near site, and they realise that the majority of workers will not have a detailed working knowledge of public photography and drone law, and such like, and consequently may react with alarm or concern at the prospect of a strange person (often in a mask) turning up unannounced to film or a drone flying over their premises (concerns that are often not without justification, it should be emphasised).

1.9. "Auditors" rely on the humiliation and personal abuse of staff to give their content appeal to viewers. In the video itself and in video titles and descriptions, "auditors" will frequently use personally abusive and insultive language to describe individuals they encounter whom they have not taken a liking to.

1.10. "Auditors" also place great reliance on their viewers and supporters, who are not passive in this. Electronic mobbing is an important aspect of "auditing", in which YouTube users who support and follow "auditing" content will add harsh and defamatory criticism of the individuals shown in a video and often call for them to be disciplined or sacked by their employers. "Auditors" often encourage their viewers to leave malicious online reviews for targeted businesses. Sometimes this is done with the encouragement of the relevant "auditor".

2. POLICY FRAMEWORK

2.1. The ACPO *Commercial Advisory Group 2010 Guidance*[144] ('2010 Guidance') was issued to inform the police approach to media generally, and the then-chair of the Commercial Advisory Group, Andy Trotter, also issued statements on public photography specifically ('the Trotter Guidance')[145]. It must be acknowledged that the 2010 Guidance and Trotter Guidance pre-date the growth of social media during the 2010s and the emergence of the "auditing" trend. "Auditing" is not public photography or vlogging, and in the majority of cases, does not involve journalism or 'citizen journalism'.

---

144 https://www.whatdotheyknow.com/request/guidanceposition_on_photography/response/685795/attach/5/CAG%20Guidance%202010.pdf?cookie_passthrough=1

145 The 2010 published guidance was preceded by a published open letter ('Guidance for Photographers') to forces from the Chair of the ACPO Communication Advisory Group: https://www.theiac.org.uk/resourcesnew/filming-in-public/ACPO_Guidance_PhotographsPublicPlaces.pdf

2.2. The 2010 Guidance and Trotter Guidance remain valid guidance for policing matters involving photography and vlogging, but generally speaking, should not be applied to the activities of "auditors" as they do not cover the trend or the nature and purpose of what "auditors" do.

2.3. This Policy and Guidance addresses the problem of social media "auditing" in its own right as a distinct trend quite separate to photography and vlogging, and is intended to sit within the existing policy framework and should be read in conjunction with the relevant Authorised Professional Practice from the College of Policing, most especially the following APPs:

- APP on Critical incident management (2013)[146]. The National decision model[147] and the Joint decision model[148] align with this APP and further guide officers, PCSOs, staff, partners and stakeholders on responses to incidents.

- APP on Conflict management (2024)[149].

- APP on Engagement and communication (2013)[150]

3. THE GENERAL RIGHT TO PHOTOGRAPH IN PUBLIC

3.1. It does remain the case that there is a common law liberty to photograph anything visible from a public right of way, including people and things on private property, with or without the consent of the owner or occupier or the person(s) being photographed. This liberty that is further enshrined in Articles 10 and 11 of Schedule 1 to the Human Rights Act 1998.

3.2. These rights are subject to law, as we will explain here, but as a general point, it is important to reaffirm something that was stated in the Trotter Guidance and applies even here: that, unnecessarily restricting photography, whether for the casual tourist or professional is unacceptable and undermines public confidence in the police service.

[146] https://www.college.police.uk/app/critical-incident-management
[147] https://www.college.police.uk/app/national-decision-model/national-decision-model?s=
[148] https://www.jesip.org.uk/joint-doctrine/the-joint-decision-model-jdm/
[149] https://www.college.police.uk/guidance/conflict-management
[150] https://www.college.police.uk/app/engagement-and-communication

4. CRIMINAL OFFENCES & CIVIL WRONGS RELEVANT TO "AUDITORS"

4.1. Most "auditing" visits involve one or more of the following offences (amongst others):

- Public order offences, contrary to sections 4A and 5 of the Public Order Act 1986.

- Harassment, contrary to section 2 of the Protection from Harassment Act 1997. The criteria in section 7(3)(a) is met simply by the auditor filming individuals without their consent in antagonistic circumstances where the individuals can be identified and do not want to be filmed (and may expressly object and/or have not given informed consent), then posting facial images online (often multiple times to the same or different social media platforms), and without any attempt to pseudonymise victims.

- Aggravated trespass, contrary to section 68 of the Criminal Justice and Public Order Act 1994.

- Being found in an enclosed yard for an unlawful purpose, contrary to section 4 of the Vagrancy Act 1824.

- Assault, contrary to section 39 of the Criminal Justice Act 1988.

- Assault by battery, contrary to section 39 of the Criminal Justice Act 1988.

- Communications offences, such as those under section 127 of the Communications Act 2003 and section 1(1) of the Malicious Communications Act 1988 and section 179(1) of the Online Safety Act 2023.

- Obstructing a constable, contrary to section 89(2) of the Police Act 1996, by deliberately acting in a suspicious manner to provoke police attention or by simulating hostile reconnaissance activity.

- Eliciting or publishing information likely to be of assistance to a terrorist, contrary to section 58A of the Terrorism Act 2000. Taking a photograph in a court building, contrary to section 41 of the Criminal Justice Act 1925.

- Taking a photograph within a prison without authorisation, contrary to section 40D of the Prison Act 1952.

- Eliciting or publishing information likely to be of assistance to a terrorist, contrary to section 58A of the Terrorism Act 2000.

- Entering, inspecting, passing over, etc. a prohibited place for a purpose prejudicial to the safety or interests of the United Kingdom, contrary to section 4(1) of the National Security Act 2023.

- Unauthorised entry to, inspecting, passing over of, etc. a prohibited place, contrary to section 5(1) of the National Security Act 2023.

- Preparatory conduct in relation to the offence in section 4(1), contrary to section 18 of the National Security Act 2023.

- Unlawful obtaining of personal data without the consent of the data controller, contrary to section 170 of the Data Protection Act 2018.

- Offence of causing nuisance or disturbance on NHS premises, contrary to section 119 of the Criminal Justice and Immigration Act 2008.

4.2. All of this is in addition to breaches of the peace in which there have been occasions when “auditors” are heard to act or speak in such a way as would put a reasonable person in fear of violence.

4.3. While not strictly police matters, the following breaches and infringements of the law are also regularly committed by “auditors”, further demonstrating their disregard for law:

- Breaches of the drone laws and regulations – including criminal offences (for instance, it is common for “auditors” to disregard the Visual Line of Sight requirements). Some of these breaches are offences could be prosecuted by the Civil Aviation Authority (CAA) (though note that sometimes local forces are called on by the CAA to pursue investigations or aid and assist through the provision of interviewing facilities, etc.).

- Virtually no “auditor” is compliant with data protection and various regulatory breaches of data protection are obvious throughout “auditing” content, including (amongst other things) failure to comply with the disclosure requirements in Article 13 of the UK GDPR and failure to register as a data controller, as required under Regulation 2 of the Data Protection (Charges and Information) Regulations 2018. These failures can attract substantial civil fines, should the Information Commissioner’s Office (ICO) elect to enforce the regulations against “auditors”.

4.4. “Auditors” also habitually commit various civil wrongs - typically including trespass of land, aerial trespass (with a drone), trespass to the

person, misuse of private information, and individual and corporate harassment. Victims of auditors –individual staff, businesses and companies – could bring civil proceedings in the courts against "auditors".

5. POWERS OF ATTESTED CONSTABLES RELEVANT TO "AUDITING"

Powers are available to police officers to deal with "auditors" and to ensure the application and enforcement of the relevant law as outlined in 4 above:

- The most fundamental power of any constable is the ancient common law power to arrest a person for a breach of the peace or for conduct that threatens or is likely to result in a breach of the peace. A breach of the peace is not in itself a criminal offence, but the power of arrest and de-arrest would serve as an effective method for officers to de-escalate incidents and disrupt and deter the activities of "auditors".

- Officers have the power under section 50 of the Police Reform Act 2002 to demand the name and address of a person engaged in anti-social behaviour. This power may form the linchpin of an 'intelligence-led' approach to tackling "auditing".

- Officers can make use of the stop and produce powers under sections 163 and 164 of the Road Traffic Act 1988.

- Article 13 of the UK GDPR requires that a data controller identify him/herself to a data subject. There is no express power to immediately enforce this in any given situation, but officers should be made aware of Article 13 because any refusal to comply could be reported by the force to the ICO and YouTube respectively, and if repeat complaints are received about the same person/content creator, either or both may then take action. The ICO in particular has the power to fine individuals for breaches of data protection and may elect to do so where it is apparent that the breaches are numerous and systematic – as they always will be on the part of an "auditor".

- "Auditors" typically operate by visiting a number of public buildings or businesses in the same vicinity. Section 34 of the Anti-social Behaviour, Crime and Policing Act 2014 gives dispersal powers for officers in a locality on the authorisation of an inspector[151]. This power could be used where it is reported that an "auditor" is operating in a given area. On invocation of the power, officers would be able to attend at the scene and require that the "auditor" should disperse on the grounds that

[151] This must be for the purpose of removing or reducing the likelihood of behaviour occurring that is likely to cause harassment, alarm or distress – see sub-section 34(2)(a) of the Anti-social Behaviour, Crime and Policing Act 2014.

he is engaging in behaviour likely to cause harassment, alarm or distress[152].

- Constables and PCSOs (if so designated) are empowered under section 43 of the Anti-social Behaviour, Crime and Policing Act 2014 to issue Community Protection Notices, which could be a useful and effective way of disrupting the activities of an "auditor" where he is operating in his own locality. A CPN must be preceded by a Community Protection Warning.

6. SUGGESTED INCIDENT MANAGEMENT GUIDANCE FOR RESPONSES TO "AUDITORS"

See the Schedule attached.

7. THE ROLE OF PCSOs

The role and powers of PCSOs will vary from force to force. PCSOs should interpret section 5 above on Powers, and the Incident Management Guidance in the Schedule, through their own roles and local designated powers, and local circumstances, and should seek further guidance and help from colleagues.

8. GUIDANCE FOR POLICE STAFF

Call handlers and dispatchers

8.1. Call handlers have an important role in ensuring effective outcomes to incidents involving "auditors", and initial diligent work by a call handler may be pivotal in this regard. It is especially important to note that when a call handler is receiving and generating a call for service concerning a suspicious subject or of suspicious activity, that the call handler should obtain facts from the informant that articulate what is suspicious or of concern. It is of equal importance that dispatchers relay these facts to responders

8.2. If the event is generated by a member of staff's observations, it is important that the primary responder clearly communicate the circumstances to other responders. Doing so will help prevent a detention being unnecessarily imposed in the event that the reason for a detention did not exist.

[152] Section 35(2) of the Anti-social Behaviour, Crime and Policing Act 2014.

Police staff who encounter "auditors"

8.3. Police staff should be briefed on "auditors". There have been incidents when unsuspecting members of police staff have been approached when entering or exiting various parts of police buildings and premises. "Auditors" will also notice any unintentional indiscretions such as defective car, uniform etc., all of which can be uploaded onto their channel. Staff should not use any type of inappropriate or offensive language when interacting with "auditors".

8.4. Staff should follow internal security procedures for their force when encountering "auditors" on police premises.

9. ORGANISATIONAL MEASURES

9.1. All police officers and staff should be briefed on this Policy and Guidance.

9.2. Forces should adopt a cognitive and cultural approach to "auditing" that recognises:

- "auditing" is not a legal activity;
- the need to embrace both enforcement and intermediate strategic initiatives; and,
- "auditing" incidents are (or potentially are) Critical Incidents, as defined in the College of Policing APP on Critical incident management.

9.3. Forces should utilise existing local partnerships and multi-agency partnerships to address concerns (if any) about "auditors", ascertain what local businesses and public bodies would expect from the police should incidents occur, and to guide local businesses and public bodies on the appropriate response to "auditors".

9.4. Forces should adopt an intelligence-led approach in co-operation and alignment with the Lead Force on this issue. Forces should ensure that:

9.4.1. officers, PCSOs and police staff report all incidents involving "auditors" to local intelligence teams for information gathering purposes;

9.4.2. assign their existing capacity of criminal analysts (or equivalent), to act as custodians of local intelligence on "auditors"; and,

9.4.3. arrange that any accumulated local intelligence should be exchanged and shared nationally with the Lead Force for this purpose, subject to data protection considerations (and the Lead Force capacity should, for its part, update local forces periodically).

9.5. All first line managers of those who are recorded by "auditors" should be informed to help manage any welfare issues that arise and forces should provide full support (including the appropriate resources) to officers, PCSOs and staff who wish to submit complaints and takedown requests to social media platforms such as YouTube.

9.6. The force's corporate communications/media department should be notified of any incidents in order to support any subsequent public confidence issues and responses that may be required.

SCHEDULE

RESPONSE MANAGEMENT FOR OFFICERS ENCOUNTERING "AUDITORS"

N.B: This Guidance must be read in light of the general Policy and Guidance issued on Social Media "Auditors", the College of Policing APPs on Critical incident management (2013), Conflict management (2024), and Engagement and communication (2013), the National decision model, the Joint decision model, and any policy and guidance pertinent to the force's statutory public sector equality duty pursuant to section 149 of the Equality Act 2010.

Role of this Guidance

1. This is guidance rather than a protocol or standard operating procedure. It is not intended to be prescriptive, nor can it be authoritative because the authority is always the officer 'on the ground' who must face what he faces and make his decision in light of what he sees and hears. In full appreciation that "auditing" is a novel trend and that no two situations will be the same, this guidance is intended to inform, guide and assist rather than suffocate or restrict the police response.

The importance of police discretion and good judgement

2. No amount of guidance can replace the common sense and good judgement of officers 'on the ground'. Police discretion is an important aspect of policing[153]. "Auditing" is not a legal activity, but even where offences or anti-

[153] "*Police officers must be allowed to police with discretion. Discretion is the bedrock of policing; it allows reasoned and fair decisions based on experience to be taken by police officers without the need to*

social behaviour are suspected in a particular incident, it is open for officers to decide that it would be proportionate and sensible to simply deescalate the incident and give words of advice rather than take the matter to law.

Responding to "auditors" you encounter

3.1. It is important to remain calm and professional if responding to a situation where someone is photographing/recording as an "auditor". It will not always be clear whether the "auditor" is committing an offence, as such, or any obvious civil wrong, and "auditors" are always looking for an inappropriate response by police or to be unlawfully detained.

3.2. "Auditors" are typically profiled as:

- white British (there are a small number from other racial and ethnic backgrounds);
- male (there is a handful of female auditors);
- aged in their 30s and 40s (though many are older or younger);
- unmarried and single (though many are in relationships);
- of low income and/or on state benefits;
- having an unskilled vocational background with few or no academic or trade qualifications, etc. (though there are "auditors" from a wide range of socio-economic backgrounds, and some have university degrees or skilled trades);
- having low levels of literacy/reading ability (some have learning difficulties);
- having mental health issues/personality disorders (given the nature of the activity, it is difficult to regard any of them as mentally normative);
- having a criminal record of some sort and/or a history of significant conflict with the law or other authority.

3.3. "Auditors" hold strident beliefs about their activities and tend to become defensive and emotional when challenged by authority. They have strong cognitive biases and strongly manifest the Dunning-Kruger effect in their understanding of the relevant general laws on photography, data protection and trespass, etc. They will strongly maintain their understanding of the law in any given area is correct, and even proceed to insult and disparage anyone who disagrees and will maintain this position even if it can be clearly shown that they have fundamentally misunderstood the law at hand. For instance,

---

take a course of action merely to satisfy targets." Page 4 of *The Office of Constable - The bedrock of modern*
day British policing, published by The Police Federation of England and Wales.
https://www.polfed.org/media/14239/the-office-of-constable-with-links-2018.pdf

most “auditors” are convinced that data protection does not apply to them at all (in fact, it does) and that they can enter private land/buildings without trespassing if the premises are publicly-accessible and/or there is no sign barring trespass (this is typically only the case if visitors are reasonably expected by the occupier).

3.4. Your first words to an “auditor” will often dictate the remainder of the contact, as with any other contact. A professional greeting such as, “How’s it going today?” will often work better than, “What are you doing out here?” or “Why are you recording [this building]?”

Information-gathering and assessment of reasonable suspicion

4.1. It is important to be honest, clear and open in your communication with “auditors”, just as with anyone you encounter in the course of your duties. For instance, if responding based on a call reporting suspicious persons, it is appropriate to say why you are there. Such a response might be similar to the following:

“Someone called regarding your activity. I would like to ask you a few questions about what you are doing out here. You are not being detained, and are free to leave at any time.”

“Some people find it suspicious and concerning that you are recording premises and staff. I would simply like to find out what you’re doing out here and also be able to reassure our community about what’s happening.”

4.2. In short, and in all scenarios, it is perfectly acceptable to conduct a simple stop and account in accordance with your force standard operating procedures, in which you ask “auditors” what they are doing, why they are recording, and what their purpose is for recording such activities.

4.3. When assessing whether there is ‘reasonable suspicion’ of an offence and/or cause for concern about non-criminal behaviour (anti-social behaviour), you should also listen carefully to what informants say about the behaviour of the “auditor” and consider the surrounding facts. “Auditors” will often cogently argue that their presence is harmless and non-threatening, but the perceptions of staff whom they are recording may be very different, and these reports may be one among other factors in informing whether there is a basis for reasonable suspicion of one or more offences.

Intelligence sharing on “auditors”

5.1. As soon as it becomes apparent from the reported behaviour of the individual(s) that you are dealing with an “auditor”, and assuming the “auditor” does not volunteer his personal details, the power under section 50 of the Police Reform Act 2002 should be utilised to obtain the name and address of the “auditor” (‘section 50 information’). This power can and should be invoked irrespective of whether there is reasonable suspicion of an offence because

"auditing" can be considered anti-social behaviour in itself – however, note paragraph 5.2 below.

5.2. The section 50 power should only be used where there is a real possibility that the individual of interest is an "auditor". This can only be left to the judgement of the officer(s) on the scene, but officers should always err on the side of giving the benefit of the doubt. Even when the belief that an individual of interest is an "auditor" seems well-founded, individuals of interest who deny they are "auditing" or refuse or fail to confirm or deny what they are up to should be afforded every opportunity to provide reassurance in explaining and demonstrating the nature of their activities.

5.3. As well as the usual 'PNC check' at the scene, the "auditor's" name and address should be checked *in situ* against any intelligence held by the local force to confirm the general background and nature of the "auditor's" social media activities. This local intelligence product should include the name and address of the "auditor", the name of any social media channels that the "auditor" operates, a physical description and image stills of the "auditor", and any other relevant information, and should be available to response officers to peruse on their secure devices. This intelligence should clarify and inform any immediate decision about how to escalate/deescalate the incident, as the case may be.

Incident decisions in loco and suggested outcomes

6.1. If you do have grounds for reasonable suspicion or otherwise have grounds to believe the "auditor" has committed anti-social behaviour or behaviour that may otherwise represent a genuine security risk or risk to the personal information of staff that could be misused, you should be clear and confident of the powers at your disposal, and clearly articulate why you are using them. Do not seize a camera or phone unless you deem it evidential.

6.2. Consider the appropriate escalation, which could be one or a combination of the following (in conjunction with the use of section 50 powers, as outlined in 5 above):

<u>Simple de-escalation</u>
This may be the appropriate outcome where it is not apparent that the "auditor" is committing an offence, any anti-social behaviour is of a trivial nature, and the "auditor" is prepared to co-operate in the resolution of any immediate civil infraction such as simple trespass. It is then a matter for the occupier to pursue civil remedies against the "auditor", as the case may be.

<u>Words of advice</u>
This may be the appropriate outcome where it is apparent that the "auditor" has committed offences or significant anti-social behaviour, but the informant is reluctant to go to law.

Anti-terrorist suspicion-based stop and search

The stop and search power in section 43 of the Terrorism Act 2000 should be used only when reasonable suspicion exists that an article relating to terrorism will be found. The appropriate use of this power is therefore likely to be restricted to incidents in which the actions of the "auditor" bear similarity to what that may be expected of a terrorist (see discussion of ***simulating suspicious behaviour*** and ***simulated hostile reconnaissance*** in paragraph 1.7 of the main Policy and Guidance). Note furthermore that it is unlikely a routine suspicion-based stop and search under section 1 of the Police and Criminal Evidence Act will be appropriate or relevant to very many "auditors", given the type of offences involved.

Diversion

This may be an appropriate outcome in combination with one or more of the other outcomes where the "auditor" has obvious social vulnerabilities or manifestly has severe mental health issues. Officers may refer the "auditor" to Liaison and Diversion (L&D) services within the local NHS. Consideration should also be given in these circumstances to using powers under section 136 of the Mental Health Act 1983 if it is felt that the individual is suffering from acute mental ill-health and in immediate need of care and control. It is suggested to seek the advice of a clinician in advance to ascertain if the individual is known to local mental health services and receiving care or treatment.

Dispersal

"Auditors" typically operate by visiting a number of public buildings or businesses in the same vicinity. Section 34 of the Anti-social Behaviour, Crime and Policing Act 2014 gives dispersal powers for officers in a locality on the authorisation of an inspector. This power could be used where it is reported that an "auditor" is operating in a given area. On invocation of the power, officers would be able to attend at the scene and require that the "auditor" should disperse. Where applicable, this may be the appropriate outcome in conjunction with one or more other outcomes listed here.

Issuance of a Community Protection Notice

This may be an appropriate outcome where the "auditor" is operating in his own locality. A CPN must be preceded by a Community Protection Warning.

Report for summons

This may be the appropriate outcome where the "auditor" has committed one or more offences and the officer decides that it is likely there is sufficient evidence available to bring a prosecution without the need to arrest the "auditor" and/or seize and interrogate the "auditor's" equipment and it is otherwise not necessary to arrest the "auditor" for any other reason.

Arrest and de-arrest

This may be an appropriate outcome for the purpose of ending or preventing a breach of the peace at the scene.

Arrest and detain

This may be the appropriate outcome where the “auditor” has committed one ore more offences and the officer decides that it is necessary to arrest the auditor and/or it is likely that material evidence that will aid a further investigation is stored on the “auditor’s” equipment, which must be seized and interrogated. A general power of arrest is contained in section 24 of the Police and Criminal Evidence Act 1984, which may be used for the purpose of preserving evidence (i.e. the ground in sub-section 24(5)(e))..

6.3. In regard to searches and interrogations of electronic devices, whether in situ or to aid a formal investigation, it is important to note that once an image has been recorded, the police have no power to delete or confiscate it without a court order.

Words of advice and other action in respect of victims/informants

7.1. Allowing for what we say in 7.2 below, officers should be careful as far as practicable to avoid any action that appears to appease or side with the “auditor”, such as giving words of advice or guidance to the occupier in front of the “auditor”.

7.2. Where it appears the “auditor” has a bone fide criminal complaint against the occupier or member of staff, this should obviously be dealt with in the normal manner and need not be covered by this guidance.

Supervision of self-help remedy

8.1. All occupiers and their agents are availed of the common law self-help remedy of physical ejectment of a trespasser. The role of the police if called to attend in these situations is to monitor and supervise the conduct of physical force to ensure that the force used is lawful, that there are no offences, and to otherwise keep the peace.

8.2. It is not within the scope of the duties of a constable to act as agent for the occupier in the exercise of force. Therefore, officers should intervene in the exercise of self-help only to the extent that is within their duties as outlined in 8.1 above.

Suggested post-incident procedures

9. In addition to standard operating procedures relating to arrest and custody (if applicable), and regardless of outcome or action/no action, the PNC and any other local intelligence product should be updated with the relevant information about criminal and non-criminal actions on the part of the “auditor” during the relevant incident. Local intelligence should also be updated with image stills of the “auditor” from body worn footage.