

BRIEFING: CONTROLLING THE UK'S PRIVATE INTELLIGENCE INDUSTRY

May 2022

privacyinternational.org

ABOUT PRIVACY INTERNATIONAL

Governments and corporations are using technology to exploit us. Their abuses of power threaten our freedoms and the very things that make us human. That's why Privacy International campaigns for the progress we all deserve. We're here to protect democracy, defend people's dignity, and demand accountability from the powerful institutions who breach public trust. After all, privacy is precious to every one of us, whether you're seeking asylum, fighting corruption, or searching for health advice.

So, join our global movement today and fight for what really matters:
our freedom to be human.

creative commons

Open access. Some rights reserved.

Privacy International wants to encourage the circulation of its work as widely as possible while retaining the copyright. Privacy International has an open access policy which enables anyone to access its content online without charge. Anyone can download, save, perform or distribute this work in any format, including translation, without written permission.This is subject to the terms of the Creative Commons Licence Deed: Attribution-Non-Commercial-No Derivative Works 2.0 UK: England & Wales. Its main conditions are:

- You are free to copy, distribute, display and perform the work;
- You must give the original author ('Privacy International') credit;
- You may not use this work for commercial purposes;
- You are welcome to ask Privacy International for permission to use this work for purposes other than those covered by the licence.

Privacy International is grateful to Creative Commons for its work and its approach to copyright.

For more information please go to www.creativecommons.org.

Photo by Craig Whitehead on Unsplash

Privacy International
62 Britton Street, London EC1M 5UY, United Kingdom
Phone +44 (0)20 3422 4321

privacyinternational.org

Privacy International is a registered charity (1147471), and a company limited by guarantee registered in England and Wales (04354366).

BRIEFING: CONTROLLING THE UK'S PRIVATE INTELLIGENCE INDUSTRY

May 2022

TABLE OF CONTENTS

INTRODUCTION 5

WHO 6

PRIVATE INVESTIGATORS 6

CORPORATE INTELLIGENCE AGENCIES 7

PR AGENCIES & "REPUTATION MANAGEMENT" COMPANIES 10

CURRENT REGULATIONS 12

DATA PROTECTION 12

LICENSING REQUIREMENTS 14

UNLAWFUL INTERCEPTION AND UNAUTHORISED ACCESS TO COMPUTERS 15

REFORMS NEEDED 17

DATA PROTECTION LAWS 17

LICENSING REQUIREMENTS 19

CONCLUSION 20

ENDNOTES 21

INTRODUCTION

Digital techniques traditionally exercised by state intelligence agencies to spy and spread propaganda are increasingly available on the private market to anyone with the means to pay.[1] The UK has become a global hub for this burgeoning industry, offering individuals, corporations, and foreign government agencies access to an extensive range of powers without meaningful scrutiny or safeguards aimed at preventing abuse.[2]

From reports detailing the hacking of government representatives and extensive monitoring of environmental and human rights defenders to the fabrication of campaigns on social media, these private intelligence actors comprised of hundreds of companies from traditionally different sectors have one thing in common: secrecy.[3] Promising their clients complete discretion[4] and under no obligation to provide any transparency, little is publicly known about this industry

Yet, despite high-profile scandals, overwhelming evidence, and government commitments, outlined in this briefing, it is an industry that is out of control: posing significant threats to the rights, work and safety of rights defenders, environmental campaigners, journalists, and others in the UK and abroad.

The UK Government could easily regulate this industry and stop this abuse, as other countries have done. It must now immediately prioritise regulations aimed at holding the private intelligence industry to account.

WHO

The UK's modern private intelligence industry emerged from different sectors which have all embraced digital techniques to gather intelligence and spread propaganda.[5] This includes private investigators, corporate intelligence companies, PR agencies, and "reputation management" agencies.

PRIVATE INVESTIGATORS

In contrast to other countries including Australia, Canada, New Zealand the US, private investigators are unlicensed in the UK.[6] The sector remains a free-for-all in which "Virtually anyone can charge for investigation services"[8], according to the Association of British Investigators (ABI), a voluntary standards body.

Private investigators played a central role in the UK's 'phone hacking' scandal, including by illegally intercepting voice messages and passing them to news media.[9] More recently, the far-right figure Tommy Robinson hired a private investigator to obtain the private address of a journalist working on a story about him, and then turned up at her home.[10]

While the ABI lists 311 investigators as members, with anyone free to advertise private investigative services there are unknown numbers operating in the UK and offering their services abroad.[11] Another industry association, the World Association of Professional Investigators, lists over 100 in the UK.[12]

Private investigators market themselves extensively and are prominent online. ISG, the Investigation and Surveillance Group, for example, which markets the use of video and audio recorders as well as undercover agents, promises investigators "experienced in devising strategy, executing with discretion and expertise and working across the world, wherever they're needed."[13]

CORPORATE INTELLIGENCE AGENCIES

According to the Voice of America, London's location as a hub between Asia and the Americas and history as a centre of espionage has meant the growth of a booming private corporate intelligence sector estimated to be worth $19 billion.[14]

Such companies, who unlike more traditional and smaller private investigators focus more on corporate clients around the world, offer investigative services for things like gathering intelligence on adversaries, including activists, and intelligence to be used during litigation proceedings.

Case Study: Black Cube

London-based Black Cube markets itself as a "select group of veterans from the Israeli elite intelligence units that specialises in tailored solutions to complex business and litigation challenges."[15] Claiming to have operated in over 70 countries[16], Black Cube collects intelligence for corporate clients to be used for "deep" due diligence as well as evidence in courts or as part of negotiations with adversaries.

Black Cube markets its litigation support services for clients looking to identify "opponents' vulnerabilities, interests, priorities and strategy", as well as their "sensitive points or vulnerabilities, or evidence of their misconduct."[17]

The firm gained notoriety following reports that it had been contracted by Harvey Weinstein to stop the publication of news articles detailing sexual misconduct allegations, and for reportedly "using false identities to befriend women accusing the movie titan of sexual misconduct and extract information from them."[18]

Two Black Cube employees were sentenced in Romania for attempting to hack into the emails of the country's head of anticorruption at the behest of a former senior intelligence official.[19] Haaretz reports that the techniques employed appeared to include the production of fake news stories designed to solicit responses from the family and friends of the official, Laura Kovesi, and the sending of emails with malicious attachments designed to extract data from the target if opened.[20] In February 2022 Black Cube's leadership entered into a plea agreement in Romania admitting spying on Laura Kovesi, who is now the European Chief Prosecutor.

Documents obtained by the New Yorker appear to demonstrate that Black Cube operatives had also sent emails to the family of senior advisors to President Obama and potentially formulated detailed dossiers on them having been instructed to find damaging details on them in order to undermine the 2015 Iran Nuclear Deal.[21]

In December 2021, Facebook reported[22] that it had removed around 300 Facebook and Instagram accounts linked to Black Cube, which it believed would be used "to set up calls and obtain the target's personal email address, likely for later phishing attacks". Facebook's investigation found its customers included "private individuals, businesses, and law firms around the world", and targeting "NGOs in Africa, Eastern Europe, and South America, as well as Palestinian activists".

Other high-profile corporate intelligence agencies include Welund, set up in 2007 by a former agent of UK secret intelligence service MI6 and which focuses on "monitoring and identifying politically-based threats to businesses."[23] In 2021 OpenDemocracy reported that the firm has been providing email updates about a peaceful climate protestor to oil giant BP, including CCTV footage and information about his social media activity.[24] Welund's North American operation, which markets its services to the oil and gas industry and on "understanding the

activist threat", appears to have provided intelligence on Greenpeace, Occupy Wall Street, and animal rights advocates, according to Mother Jones.[25]

Another high-profile UK firm, Hakluyt, was in 2021 accused of having used an infiltrator to gather information on Greenpeace activists after being hired by BP and Shell (both firms deny knowing the techniques employed by Hakluyt).[26]

Hakluyt last year generated a record revenue of £67.2 million and lists Sir Ian Lobban, the former director of the UK signals intelligence agency GCHQ as an advisor.[27]

Former intelligence officers also started Diligence, a London-based firm which boasts "worldwide coverage" and expertise in covert surveillance, digital forensics, and cell site analysis.[28] A 2021 expose by the Bureau of Investigative Journalism and New York Times found that the head of Diligence had tried "to pay a potential witness to testify against an enemy of President Vladimir Putin of Russia" in France in 2017, while working with legal firm Hogan Lovells. As the Bureau explains, judges in England have broad latitude to accept evidence in private-party civil proceedings, with lawyers and private investigators in London as a result "raking in huge fees and engaging in questionable tactics in the service of autocratic foreign governments."

PR AGENCIES & "REPUTATION MANAGEMENT" COMPANIES

PR companies have for long monitored and manipulated social media and other online spaces to further the interests of their clients.[29] The increasing focus on online spaces has however blurred the lines between PR agencies and intelligence companies who specialise in surveillance and propaganda techniques.

One such company is CT Group, the high-profile PR agency founded by political consultants Sir Lynton Crosby and Mark Textor. The firm[30] markets the mitigation of reputational threats by "search engine management, digital asset management, social media monitoring, dark web surveillance and cybersecurity assessment."

In 2019, an investigation by Guardian Australia reported that CT Group ran a covert "astro-turfing" campaign, in which it appears to have been paid millions by multinational mining giant Glencore to run "a secret, globally coordinated campaign to prop up coal demand by undermining environmental activists, influencing politicians and spreading sophisticated pro-coal messaging on social media." According to the Guardian, in addition to collecting intelligence about environmental activist groups and on issues which could embarrass and undermine them, the firm also appears to have set up social media content aimed at promoting "clean coal" and attacking renewables.[31]

Other companies come from backgrounds more traditionally associated with intelligence.

K2 Integrity for example, whose London office[32] focuses on business clients from Europe, Middle East and Africa, provides "Reputation Defense" services. K2 Integrity promise that by "leveraging an array of investigative methods and tools ranging from sophisticated cyber forensics to source intelligence gathering and public records analysis, we identify compelling evidence to expose the sources of misinformation, the instigators and facilitators of the smear campaign, and other

material that can be harnessed to support the client's legal and public relations response."

In 2018, K2 Integrity paid damages to five anti-asbestos campaigners after it reportedly paid an infiltrator to pose as a sympathetic documentary filmmaker who recorded conversations and passed information about the campaigners to clients in the asbestos industry.[33]

Another high-profile firm with a substantial London office, Kroll, markets "Digital Risk Protection" which "can help minimize exposure in highly politicized or activist-prone environments, especially with NGOs"[34] and monitor social media profiles.[35]

London-based SIGWATCH[36] explicitly aims to monitor activists for corporate clients, claiming to monitor "the campaigns of some ten thousands activist groups across the world to help companies see what issues are coming their way and how their industry peers are being targeted." According to SIGWATCH, it provides "subscribing organisations real-time intelligence on when, where, why and how it or its competitors are being targeted or criticized by activists, almost anywhere in the world", and provides "bespoke research" into campaign groups.

Another London-based firm, Transmission Private, also advertises "monitoring and gathering intelligence on an activist-driven campaign that was being waged on social media against a London private equity investor" as part of its reputation management services.[37]

CURRENT REGULATIONS

The range of activities described in the previous section has the potential to interfere with the privacy and other human rights of targeted individuals.

Depending on the technique employed, different legal regimes apply in the UK, most notably the Data Protection Act 2018, the Computer Misuse Act 1990 and the Investigatory Powers Act 2016.

DATA PROTECTION

Since 1st January 2021, the UK GDPR sets out the key principles, rights and obligations for most processing of personal data in the UK, except for law enforcement and intelligence agencies which are regulated by Part III and IV of the UK Data Protection Act respectively.

One of the core provisions of the UK GDPR requires that private investigators and other actors described in the above section, or most likely their clients, have a lawful basis for processing the personal data of individuals. Out of a closed list of 6 possible bases, the basis they would most likely seek to rely on is that they have a "legitimate interest", such as investigating suspected wrongdoings of business partners – but they would also need to demonstrate that such legitimate interest is not overridden by the interests or fundamental rights and freedoms of individuals being investigated. This is a difficult legal basis to establish, and most likely inappropriate in this context, and would not apply if for instance a firm were monitoring human rights defenders. Another considerable hurdle for private investigators and their clients is the requirement to inform people that they're processing their personal data – owing to the nature of their business, this is obviously difficult. The only exceptions to individuals' right to

information apply mostly in cases where informing the individuals would prejudice police investigations or other important tasks of public bodies, or will fall under exemptions e.g. for journalism, public interest archiving, or social work – none of these apply here.

While enforcement has been sporadic, the UK regulator for data protection and privacy, the Information Commissioner Office (ICO), has in the past targeted investigators and their clients for breaches of the UK data protection legislation.[38] It has also issued guidance to the public about disclosure of information to private investigators.[39]

Further, there are criminal offences in the DPA 2018 which are relevant to some of the activities described in section 1 above.[40]

Under Section 170 it is an offence for a person knowingly or recklessly to obtain or disclose personal data without the controller's consent and to procure the disclosure of personal data to another person without the controller's consent. Similarly, it is an offence for a person to sell, or offer to sell, personal data that has been, or will be, obtained unlawfully.

Under Section 171, it is an offence "for a person knowingly or recklessly to re-identify information that is de-identified personal data without the consent of the controller responsible for de-identifying the personal data."

According to the ICO, these crimes could cover "blagging (obtaining private or confidential information by impersonation or another method), hacking, or other covert methods."[41]

The UK GDPR applies to processing carried out by companies operating within the UK. It also applies to organisations outside the UK that offer goods or services to individuals in the UK, or that monitor the behaviour of individuals in the UK. Consequently, companies in the UK must comply with the UK GDPR even when they are processing personal data of individuals outside the UK – and companies outside the UK must comply with the UK GDPR if they are processing data of individuals in the UK. Therefore, even if a UK firm were to process data of individuals abroad for a foreign client, UK data protection legislation still applies.

LICENSING REQUIREMENTS

Unlike in the USA, Canada, Australia, New Zealand, Ireland and other EU countries, in the UK, there is no mandatory licencing for private investigators.

The Private Security Industry Act in May 2001 established the Security Industry Authority (SIA), a regulating body tasked to issue individual licenses to the wider security industry.[42] Private investigators can apply for a license to the Security Industry Authority (SIA) in a process described as "fairly straightforward"[43] which do not seem to involve significant background checks.

Following the News Of The World phone hacking scandal in 2013, the government committed to regulate the industry and the then Home Secretary Theresa May promising to make "it a criminal offence to operate as a private investigator without a licence."[44]

A government review published in June 2018 (Security Industry Authority Review) argued that regulation of the Private Sector Industry is needed. Specifically in relation to private investigators, the review concluded that "there is therefore a case for introducing regulation" in the form of licensing requirements.[45]

However, no such regulation has been implemented nor is it forthcoming. Even despite support from professional associations such as the Association of British Investigators (ABI)[46], the Security Industry Authority (SIA) confirmed to Privacy International in March 2022 that no regulation has been proposed or implemented and that there are no plans relating to the regulation of private investigators.

UNLAWFUL INTERCEPTION AND UNAUTHORISED ACCESS TO COMPUTERS

In a somewhat piecemeal way, UK legislation criminalises a range of activities related to unlawful interception of communications, hacking of devices and other conducts amounting to interference in someone's communications or devices.

In particular, the Investigatory Powers Act (IPA) 2016[47] criminalises unlawful interception of communication in the course of its transmission, including via a public or private telecommunication network or a public postal service. The offence requires inter alia that the interception is carried out in the UK (see Section 3). The definition of interception makes it clear that it applies to content of a communication that is not public.

Some sections of the previous investigatory powers legislation, the Regulation of Investigatory Powers Act (RIPA) 2000[48], are still in force and regulate activities like covert and intrusive surveillance, or access to encrypted information.

Section 1 of the Computer Misuse Act (CMA) 1990[49] criminalises unauthorised access to computer material. The definition is purposefully broad to include causing "a computer to perform any function with intent to secure [unauthorised] access to any program or data held in any computer, or to enable any such access to be secured".

The Act applies if there is at least one 'significant link' with the 'home country' (i.e. the UK) (See Section 4).

"A significant link could include:

- The accused is in the home country at the time of the offence
- The target of the CMA offence is in the home country
- The technological activity which has facilitated the offending may have passed through a server based in the home country"[50]

The CMA 1990 could apply to several activities performed by the private investigation organisations, such as hacking and sending emails with malicious attachments designed to extract data from the target if opened. However, at the same time, a number of activities would not fall under the Act, such as the monitoring of social media.

REFORMS NEEDED

Although some activities of the private intelligence industry can fall within the regulations outlined above, many activities are not regulated (let alone prohibited) in the UK.

Data protection and licensing requirements should be prioritised.

DATA PROTECTION LAWS

While relevant data protection laws in the UK already govern many activities undertaken by the wider private surveillance industry, there is significant scope for further attention and enforcement activities by the UK's data protection regulator, the ICO. For example, the ICO should prioritise a Code of Practice for the wider industry, which should include not only the activities traditionally associated with private investigators, but those which may brand themselves as PR and corporate intelligence agencies.[51]

Further, it should monitor revelations that describe unlawful processing of personal data by UK companies of persons located abroad, particularly as those persons are unlikely to be aware of their data rights or make complaints to the UK regulator.

The ICO should also clarify current obligations and areas that currently lack sufficient protections. In particular, there is little legislation beyond the UK GDPR to limit the social media monitoring of individuals and at scale. Privacy International has unearthed the inadequate regulation surrounding the use of social media monitoring by UK local authorities and UK police forces[52] and the "exponential growth of online activity by law enforcement agencies, particularly

in relation to open source and social media" has been noted in the 2019 IPCO report.[53] Given that the similar exploitation of open source and social media monitoring by private actors is subject to even less regulation than the activities of public authorities, the ICO should clarify their obligations.

Governments and companies often argue[54] that this collection and analysis of publicly available data or of information obtained in public spaces have little impact on people's privacy. This inaccurate representation fails to account for the intrusive nature of collection, retention, use, and sharing of a person's personal data obtained from public spaces and through social media – we have a right to privacy in public spaces as well, in that people's personal information and identity cannot be exploited in ways they can't reasonably expect. The privacy intrusion is then furthered when publicly available data sets are aggregated. This was recognised by the ICO in its decision against Clearview AI[55] (a company that indiscriminately scrapes the photos of individuals from the public Internet) – the UK GDPR does protect individuals against exploitation of their information gathered from publicly available sources, but this is often misunderstood or misapplied.

There is also a potential gap in regulation of some of the privacy invasive techniques deployed by private investigative agencies and individuals. For example, according to an assessment by the Association of British Investigators, tracking of someone's vehicle by private investigators is not prohibited. "there is no current legislation that prevents the use of a GPS Electronic Tracking Device (for example on a vehicle) by an investigator in the private sector, without the consent of the owner or user of that vehicle, providing that the physical surveillance it's use supports is lawful"[56] Regulation should seek to close any such potential gaps and clarify existing obligations.

LICENSING REQUIREMENTS

As outlined above, no progress has been made in introducing a mandatory licensing regime for private investigators despite government commitments to doing so and support from industry associations.[57]

The government should prioritise introducing legislation as recommended by the Security Industry Authority Review published in 2018[58] together with a consultation on the proposed parameters. Such legislation should aim to include professional private investigators as well as those branded corporate intelligence or PR firms who typically work under contract, but also provide clear exemptions for journalists, legal professionals and researchers, as well as those who carry out private investigative services incidentally. A consultation on the proposed regime would allow the public, civil society, journalists, researchers, private investigators, and corporate intelligence firms who are concerned or likely to be affected to provide feedback on its potential impact.

CONCLUSION: TIME TO ACT

Such action to tackle the private surveillance industry is overdue. Despite glaring examples of abuse, private investigators, corporate intelligence and PR firms continue thrive in a permissive environment that has already made the UK a global hub for the industry.

Without action, they will continue to pose a threat to the rights and safety of people in the UK and people around the world, including in countries which lack basic rule of law or avenues for redress, as well as journalists and others who work to expose corruption, protect the environment, and demand accountability. The UK government's commitments to their protection must be matched by modern safeguards which reflect these modern realities. The UK cannot be allowed to continue as an offshore haven for the private surveillance industry.

ENDNOTES

1 https://www.thebureauinvestigates.com/stories/2017-12-12/inside-the-corporate-investigations-business / https://www.wired.com/story/the-murky-merits-of-a-private-spy-registry

2 https://www.thebureauinvestigates.com/stories/2017-12-12/inside-the-corporate-investigations-business / https://www.ft.com/content/1411b1a0-a310-11e7-9e4f-7f5e6a7c98a2

3 https://www.ft.com/content/1411b1a0-a310-11e7-9e4f-7f5e6a7c98a2

4 https://www.blackhawkintelligence.com/corporate-intelligence/risk-management-services/

5 https://www.thebureauinvestigates.com/stories/2017-12-12/inside-the-corporate-investigations-business

6 https://www.theabi.org.uk/assets/uploads/Policies%20and%20Guidance/Licensing/Security_Industry_Authority_Review_2016-17.pdf

7 https://www.theabi.org.uk/assets/uploads/Policies%20and%20Guidance/Licensing/Security_Industry_Authority_Review_2016-17.pdf

8 https://www.bbc.co.uk/news/uk-24894403

9 https://www.theguardian.com/uk-news/2021/oct/13/tommy-robinson-gets-five-year-stalking-ban-after-harassing-journalist

10 https://www.theabi.org.uk/membership-search?country=222&radius=10&list_map=map

11 https://wapi.org/wapi-directory/

12 https://isg-investigations.co.uk/services/short-term-investigations#services

13 https://www.voanews.com/a/london-spy-industry-private-sector/3718445.html

14 https://www.blackcube.com

15 https://www.blackcube.com

16 https://www.blackcube.com/litigation-support

17 https://www.theguardian.com/film/2020/jan/30/harvey-weinstein-black-cube-new-york-times

18 https://www.romaniajournal.ro/society-people/black-cube-file-weiner-ron-sentenced-to-2-years-and-8-months-on-probation

19 https://www.haaretz.com/israel-news/tech-news/.premium.MAGAZINE-interrogation-revealed-black-cube-ceo-suspected-of-running-crime-organization-1.9262559

20 https://www.newyorker.com/news/news-desk/israeli-operatives-who-aided-harvey-weinstein-collected-information-on-former-obama-administration-officials

21 https://about.fb.com/wp-content/uploads/2021/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf

22 http://welund.com

23 https://www.opendemocracy.net/en/opendemocracyuk/bp-paid-ex-mi6-spy-firm-to-snoop-on-green-campaigners

24 https://www.motherjones.com/environment/2018/09/welund-private-intelligence-oil-gas

25 https://www.thebureauinvestigates.com/stories/2017-12-12/inside-the-corporate-investigations-business

26 https://www.opendemocracy.net/en/opendemocracyuk/secretive-spy-firm-met-uk-minister-to-discuss-ppe-supply

27 https://www.thebureauinvestigates.com/stories/2021-06-18/the-power-of-money-how-autocrats-use-london-to-strike-foes-worldwide

28 https://www.agilitypr.com/pr-news/analysis/a-brief-history-of-media-monitoring-and-analysis

30 https://ctgroup.com/what-we-do/campaigns

31 https://www.theguardian.com/business/2019/mar/07/revealed-glencore-bankrolled-covert-campaign-to-prop-up-coal

32 https://www.k2integrity.com/en/our-offices

33 https://www.theguardian.com/world/2018/nov/08/security-firm-pays-damages-to-anti-asbestos-activists-it-spied-on

34 https://www.kroll.com/en-ca/insights/events/2021/webcast-digital-risk-protection

35 https://www.kroll.com/en/services/forensic-investigations-and-intelligence/reputational-risk/social-media-risk-assessments

36 https://www.sigwatch.com/about-us/bespoke-research/

37 https://transmission-private.com/expertise/reputation-management

38 https://www.theguardian.com/technology/2018/jan/05/insurance-firm-and-two-of-its-employees-given-record-data-breach-fines

39 https://ico.org.uk/media/1556/disclosures_to_private_investigators.pdf

40 https://www.legislation.gov.uk/ukpga/2018/12/part/6/crossheading/offences-relating-to-personal-data/enacted

41 https://ico.org.uk/media/about-the-ico/documents/4018647/journalism-code-draft-202110.pdf

42 https://www.legislation.gov.uk/ukpga/2001/12/contents

43 https://privateinvestigator.co.uk/private-investigator-license/how-do-you-get-a-private-investigator-license/

44 https://www.gov.uk/government/news/new-regulation-of-private-investigators-to-be-introduced

45 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/703258/Security_Industry_Authority_Review_2016-17.pdf

46 https://www.theabi.org.uk/assets/uploads/Policies%20and%20Guidance/Licensing%20investigation%20in%20the%20UK%20%26%20ROI.pdf

47 https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted

48 https://www.legislation.gov.uk/ukpga/2000/23/contents

49 https://www.legislation.gov.uk/ukpga/1990/18/contents

50 https://www.cps.gov.uk/legal-guidance/computer-misuse-act

51 https://wapi.org/uk-the-abi-proposal-to-the-ico

52 https://privacyinternational.org/explainer/3587/use-social-media-monitoring-local-authorities-who-target

53 https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPC-Annual-Report-2019_Web-Accessible-version_final.pdf

54 https://www.local-detective.co.uk/blog/is-vehicle-car-tracking-legal-or-illegal

55 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/11/ico-issues-provisional-view-to-fine-clearview-ai-inc-over-17-million

56 https://www.theabi.org.uk/assets/uploads/Policies%20and%20Guidance/ABI%20Tracking%20Policy%202016-08-17.pdf

57 https://www.theabi.org.uk/about/licensing-of-investigations

58 https://www.theabi.org.uk/assets/uploads/Policies%20and%20Guidance/Licensing/Security_Industry_Authority_Review_2016-17.pdf

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org

Privacy International is a registered charity (1147471), and a company limited by guarantee registered in England and Wales (04354366).