

BIG BROTHER WATCH

Classroom Management Software – Another Brick in the Wall?

How schools use software to monitor pupils

A Big Brother Watch Report

November 2016

Contents

Introduction.....	3
Key Findings.....	5
Background.....	6
Key Questions.....	10
Regional Breakdown.....	12
Appendix 1: Examples of Providers and the Capabilities they Offer.....	15
Appendix 2: Methodology.....	16
Original Freedom of Information Request.....	17

Introduction

Unless you are a teacher or have a child in school, it is likely you are not familiar with a modern classroom. Your memories of school may be of chalk boards and scribbling down lessons in a workbook. Answering a question meant putting your hand up, whilst talking to a friend, or enemy, was done by scrawling on scraps of paper. Information came from books and encyclopaedias not the internet, in fact the only time you may have used a computer was in a specific information technology lesson and even then there weren't enough computers for every student to have a go.

That vision of school is already out of date and will soon be obsolete. The analogue classroom of old has been replaced with smartboards, internet connected devices and communication via instant message. And rightly so. Learning in the 21st century must revolve around technology in order to teach children the skills required for a digital life in a digital society.

The challenges of the modern classroom have changed. Ensuring that education is connected but that children aren't involved in cyber bullying, sexting or exposed to online extremism is a daily challenge for schools and teachers alike. Whilst the internet offers huge potential for learning the opportunity for distraction is never far away. Simply making sure a class is focused becomes a different proposition when pupils can work on screens hidden from the teachers gaze. So what are the options available for schools to address these concerns?

A raft of software companies have over recent years begun to offer what they see as appropriate technological solutions. Classroom Management Software is the "must have" tool schools are encouraged to buy, to help teach and monitor students in the modern classroom. Whilst Classroom Management Software can be used for a number of purposes, predominantly schools and teachers are being encouraged to use it to:

- Monitor the screens of an entire class from a single desktop;
- Monitor pupil internet activity in real time;
- Access a pupil's internet history;
- Automatically capture screenshots from a device whilst in use;
- Monitor keyboard strokes and create alerts if pupils type inappropriate or flagged words;
- Alert staff to signs of bad or inappropriate behaviour or signs of extremism and radicalisation.

Although Classroom Management Software is marketed as something that can help maintain discipline in a connected classroom, some teachers feel they are being asked to snoop on their pupils' every move.

Classroom Management Software – Another Brick in the Wall? is the third Big Brother Watch report into the use of surveillance technologies in our schools. It reveals that **72% of English and Welsh secondary schools are using this software**. Despite this the use of Classroom Management Software is little known and we would argue little understood, particularly by the pupils required to give their permission for their data to be monitored. This report seeks to shine a light on the use of the technology before it completely takes root in the modern classroom.

Finding the balance between maintaining children's security without impinging on their right to privacy is complicated. Ensuring teachers are able to teach, encourage and inspire rather than spend their lessons monitoring student's computer screens for signs of inappropriate behaviour is also critical. Classroom Management Software may have a genuine role to play. But it can only be a

legitimate role when boundaries have been set on its use after informed public debate. We are therefore publishing this report to kick-start that debate on this emerging issue.

The school environment must continue to encourage ideas, information and imagination to flourish, not be restricted by tracking, monitoring and analysing a child's every move. Modern schools must not allow themselves to become modern panopticons.

Big Brother Watch's key concerns are:

1. The use of Classroom Management Software, in conjunction with a school's use of CCTV and biometric systems risks normalising children to surveillance.
2. Schools often consider purchasing software for such laudable reasons as keeping pupils safe online, or to adhere to the Government's PREVENT strategy. But we are concerned that the use of technology which allows real time monitoring is placing teachers unwittingly in the position of being Big Brother. Forcing staff to oversee their pupils every digital move represents a fundamental shift from the traditional method of overseeing pupils by engaging with them from the front of the class.
3. Classroom Management Software can be used by teachers to monitor how devices are used by pupils. It can also be used by schools to filter and restrict access to internet websites which may be deemed as controversial or inappropriate. Schools regularly prevent access to social media sites, but concerns exist that excessive or overzealous filtering can have the unintended consequence of blocking access to legitimate educational material. Current guidance from the Department of Education offers no specific guidelines as to what is considered an appropriate level of filtering.
4. The encouragement for schools to adopt a Bring Your Own Device (BYOD) scheme could lead to further examples of this software being installed on pupils privately-owned devices and for monitoring of pupils' activity on personal devices being undertaken outside of the classroom. Use of software in this way, we believe, would be excessive and would cross the line into schools intruding into pupils' private lives.
5. Schools currently offer little explanation about the use of the software in their acceptable use policies. Pupils and parents, who have to sign such policies to say they agree to the use of the software, are therefore left completely in the dark. In May 2018 the General Data Protection Regulation is set to replace the Data Protection Act 1998. Schools will have to obtain informed consent from pupils and parents (if the pupil is under 16) before any data is collected. Without a complete overhaul of current practice, schools will be in breach of data protection law.

Key Findings

- **1420 (44%)** of the **3259** Secondary schools we sent a Freedom of Information request to responded.
- **1000 (70%)** of responding Secondary schools in England and Wales use a Classroom Management Software package.
- Classroom Management Software has been installed on:
 - **821,386** devices; computers, laptops, tablets or mobile phones
 - **819,970 (99.8%)** school owned devices
 - **1416 (0.2%)** pupil owned devices
- In total **£2,521,051.03** has been spent on Classroom Management Software by those schools. Costs increase every year due to annual maintenance or subscription fees.
- The three largest suppliers of Classroom Management Software are:
 - Impero used by 403 schools.
 - AB Tutor used by 160 schools.
 - RM Education used by 108 schools.
- Out of **1000** schools, only **149 (15%)** provided us with Acceptable Use Policies. Of those 149 schools:
 - **26 (17%)** gave detailed information about the type of Classroom Management Software and how it was used.
 - **123 (83%)** failed to give any information beyond the fact that students may be monitored when using computers.

Background

What is Classroom Management Software?

Classroom Management Software is software designed to assist teachers in classrooms where students predominantly work on connected devices such as computers, laptops or tablets.

Classroom Management Software can be used to:

- Monitor the screens of an entire class from a single desktop;
- Monitor pupil internet activity in real time;
- Access a pupil's internet history;
- Automatically capture screenshots from a device whilst in use;
- Monitor keyboard strokes and create alerts if pupils type inappropriate or flagged words;
- Alert staff to signs of bad or inappropriate behaviour or signs of extremism and radicalisation.

A list of some of the leading providers and some of the capabilities their software offer can be found in Appendix 1.

Are schools required to use Classroom Management Software?

Use of Classroom Management Software is a choice. However, schools may be encouraged to purchase the software in order to adhere to their obligations under the Government's PREVENT Strategy¹ or as a way of following the Keeping Children Safe in Education guidance published by the Government in September 2016².

The software is also marketed as a way schools can tackle the problems of cyber-bullying, sexting, self-harm, or as a way of identifying pupils who may be having suicidal thoughts. The words pupils type whilst using a device can be monitored and run against a "keyword abuse library" to flag issues of concern.

Under the Government guidance, schools are informed that *"it is essential that children are safeguarded from potentially harmful and inappropriate online material"*³ and that *"children are safe from terrorist material."*⁴

The guidance goes on to say that *"Whilst it is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place, they should be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."*⁵ However no definition as to what is considered "appropriate" is given.

Have concerns been raised about the use of monitoring or filtering in schools?

Concern about the lack of clarity and definition in the Government guidance were raised during the Government's consultation process. 87% of the schools and colleges said that they wanted guidance on what *"appropriate" filters and monitoring systems look like* and *"advice on how to satisfy themselves that they have them."*⁶

1 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97976/prevent-strategy-review.pdf

2 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/550511/Keeping_children_safe_in_education.pdf

3 Ibid.

4 Ibid.

5 Ibid.

6 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/526157/Keeping_children_safe_in_education_govt_response_26_May_2016.pdf

Respondents also stressed that *“educating pupils about staying safe online was...just as important as the use of filtering and monitoring software”* and that *“There is a risk of over-blocking of legitimate sites which pupils may be using to find educational material.”*⁷

Concern was expressed by the National Union of Teachers regarding the use of monitoring technology, with worries making the headlines that teachers will be required to act as *“a front-line storm trooper to listen, to spy on and to inform the authorities of students we may be suspicious of.”*⁸

Russell Hobby, General Secretary of the National Association of Head Teachers warned that this kind of role is not something that teachers are familiar with, noting *“the idea of conducting surveillance on students or taking on some sort of policing of students is alien to schools.”*⁹

Teachers regularly stress that there is little evidence that children are radicalised whilst at school. This has been emphasised by Christine Blower, the former National Union of Teachers General Secretary, who has said that *“Evidence shows that grooming by extremist groups happens mainly on social media sites, not on school premises.”*¹⁰ This view was mirrored by the head teacher at Bethnal Green Academy, the school where the three schoolgirls who flew to Syria to join ISIS were educated, who said at the time that *“police have advised us that there is no evidence that radicalisation of the missing students took place at the academy.”*¹¹

What information is given to pupils and parents about the use of Classroom Management Software?

Schools are advised to issue acceptable use policies to students. These documents have to be signed by the pupil and/or by the parent or guardian to confirm that they are happy to adhere to the policy of the school when it comes to using technological devices and the internet as part of their studies in school.

83% of the policies provided to Big Brother Watch in response to our Freedom of Information requests contained no real information about Classroom Management Software. Of the 10% who did mention the software, it was either referred to in very basic terms, such as *“I know that the school can remotely monitor what I can do on the computers”*, or more intimidating language was used, with a couple of schools warning students that they are *“NOT invisible”* or that they are *“being monitored”*. This is not only inappropriate but in most cases the schools are failing to adhere to data protection law.

Schools must ensure that pupils and parents know what is happening with their data and why their data is being monitored. Data protection law is changing. By May 2018 any organisation handling data must ensure they inform the individual exactly why their data is being gathered, used, shared or monitored. Only then can the individual be sure to have given their informed consent to the use of their personal data.

We note that a blog on the Impero website has been published which alerts schools using their software about the changes in data protection law. The blog states that schools should *“Review how the school seeks and records consent for the processing of personal data and consider any changes*

7 Ibid.

8 <http://www.independent.co.uk/news/education/education-news/teachers-forced-to-act-as-front-line-storm-troopers-to-spy-on-pupils-under-guidelines-aimed-at-10158043.html>

9 <https://www.theguardian.com/education/2015/jun/09/schools-duty-police-extremism-anti-terrorism-laws>

10 <https://www.theguardian.com/politics/2016/mar/28/teachers-nut-back-motion-calling-prevent-strategy-radicalisation-scrapped>

11 <https://www.tes.com/news/school-news/breaking-news/missing-bethnal-green-academy-students-not-radicalised-school-site>

required as part of these new Regulations.”¹² We welcome Impero’s approach and would like to see similar engagement from other developers of this software.

Is Classroom Management Software secure?

As cyberattacks, hacking and malware become a common problem the need to maintain the highest levels of security is absolutely critical. Schools must be reassured that the products they are purchasing and installing are adhering to the strictest security standards.

Reports of problems with security of Classroom Management Software have appeared in the press. In 2015 a security researcher discovered a profound vulnerability running on the Education Pro software produced by Impero Solutions¹³. This could have allowed the installation of spyware or access to files and records. The company released a patch, but the incident highlights that the safety of children isn’t solely about protecting them from searching for, viewing or typing inappropriate words and images. It also involves ensuring that the personal information held about them and their education is properly secured.

Is Classroom Management Software installed on pupils’ personal devices?

Currently, the majority of schools using the software are installing it on school-owned devices only. However many schools are being encouraged to adopt a Bring Your Own Device (BYOD) scheme. BYOD allows a pupil to use their own personal device at school for school work rather than use a school device. Schools are also encouraging 1:1 schemes, where every pupil is assigned the same school owned device whilst they are at that school.

We have discovered that already over 1400 pupils’ personal devices have been installed with Classroom Management Software. We imagine this to be just the start of a growing trend.

Developers of the software will no doubt be keen to ensure that BYOD devices are secured by their software and schools will want to know that personal devices aren’t going to interfere with their networks. For example, Impero’s mobile monitoring software¹⁴ can be installed onto pupils’ own devices enabling teachers to monitor or the school to restrict access to specified websites. It is not clear, based on the information provided by Impero, if the software is only activated when pupils are in class using their device to study, when pupils are on school property, or if it remains activated when pupils are off-site during evenings, weekends and school holidays.

Recent evidence given to the Lords Select Committee on Communications revealed that a monitoring system called e-Safe can be installed on school owned devices which are permitted to be taken home during evenings, weekends and school holidays. Whilst e-Safe isn’t marketed as a Classroom Management System, but as a “*monitoring service*”¹⁵ the capability of the software is similar.

Mark Donkersley, Managing Director of e-Safe¹⁶, said in the evidence session that: “*we are doing this throughout the year, the behaviours we detect are not confined to the school bell starting in the morning and ringing in the afternoon, clearly; it is 24/7 and it is every day of the year.*”¹⁷

12 <https://www.imperosoftware.co.uk/is-your-school-ready-for-the-new-eu-data-protection-regulation/>

13 <https://www.theguardian.com/technology/2015/jul/14/security-flaw-found-in-school-internet-monitoring-software>

14 <https://www.imperosoftware.co.uk/byod-mobile-device-management-software/>

15 <https://www.esafeeducation.co.uk/>

16 Of the schools which responded to our FOI two reported using e-Safe Education products.

17 <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/communications-committee/children-and-the-internet/oral/41158.html>

Whilst e-Safe make clear on their website that their technology is monitoring “*school owned devices ...constantly, even when offline...24/7, 365 days a year*”¹⁸ the other companies we have researched are less precise or forthcoming.

The broad lack of detail provided by software developers on their public-facing websites about the extent this software can be used is of concern. The failure of schools to explain to pupils and parents when the software is and isn't activated by providing them with adequate acceptable use policies is equally worrying.

Although well-intentioned, the provision of a school device monitoring on and offline engagement 24/7, 365 days a year challenges the idea of Article 8 of the Human Rights Act 1998. This stipulates that every person should be afforded the right to a private family life. In addition the failure to inform pupils will breach the General Data Protection Regulation which will be law by May 2018.

What other forms of surveillance take place in schools?

Our previous reports have raised awareness of the use of CCTV and biometrics in schools. In our 2012 report *The Class of 1984*¹⁹ we found that 90% of English, Scottish and Welsh schools had at least 1 CCTV camera on their premises, and 206 schools were found to have installed cameras in changing rooms and bathrooms.

In total in 2012 we found that 47,806 CCTV cameras had been installed by schools. We can only imagine that this number has increased. It is staggering that schools have installed more CCTV than the 45,284 cameras controlled by local authorities²⁰.

Our 2014 report *Biometrics in Schools*²¹ found that 40% of schools in England used fingerprint biometric systems for keeping track of library books or allowing cashless lunch systems to operate. The report found that a third of schools had failed to obtain parental consent before introducing the systems; this was before the Protection of Freedoms Act 2012 made such consent mandatory.

18 <https://www.esafeeducation.co.uk/our-solution/>

19 https://www.bigbrotherwatch.org.uk/files/school_cctv.pdf

20 <https://www.bigbrotherwatch.org.uk/wp-content/uploads/2016/02/Are-They-Still-Watching.pdf>

21 https://www.bigbrotherwatch.org.uk/files/school_cctv.pdf

Key Questions

Our research has revealed a number of grey areas and unanswered questions about how this software is used in schools. Whilst it is necessary that schools protect children during their education, using software to achieve this may not be the only solution. A properly informed debate is urgently needed, across the whole of society, about what level of monitoring of our children is acceptable. Without an open, transparent and honest conversation, where the benefits and concerns are discussed equally, we could be instilling surveillance as a certainty in the lives of today's youth and in the lives of future generations.

So in order to begin this process of discussion, we pose a number of critical questions which should be answered as the first step towards a healthy debate about monitoring in modern education.

Consent:

Pupils and their parents have to understand how this software will be used and how it will impact on their learning. Acceptable use policies, which must be signed by pupils, are the ideal way of ensuring information is communicated both to pupils and parents alike.

- How and why is the school using the software?
- What are the full capabilities of the software?
- What type of websites or terms may be flagged by the software?
- Will the school provide details of any significant updates to the software?

Retention:

Many of the features of Classroom Management Software require information about pupils to be stored. It is important that any retention of data is done in a clear and transparent way.

- Who has access to the information collected by Classroom Management Software?
- Can pupils and their parents see the information that has been stored about them in the same way they can access school records?
- Can this recorded data impact permanent school records?
- What data can and will be shared with other authorities?

Safeguards:

Schools have to understand what they should be doing to keep children safe, but this needs to be balanced with the ongoing encouragement of pupils to learn and develop opinions on controversial or sensitive issues.

- What systems are schools required to have in place to meet government guidelines?
- Are schools being encouraged by the Government to educate about cyber awareness and safety online or are they being encouraged just to monitor activity?
- Are pupils encouraged to talk and report problems or is the use of monitoring software overriding traditional methods of dealing with problems?

Security:

Barely a week goes past without a new high-profile hack or data breach. Schools are not exempt from this pattern and must ensure they are fully protecting themselves against cybercrime.

- Are schools properly prepared to cope with serious cyber-attacks?
- How well is pupil data being protected?
- Are software providers doing enough to protect all schools with security updates even if they aren't paying for ongoing support?
- Do schools know exactly when and where to report a threat or breach?

Bring Your Own Device:

As BYOD or 1:1 schemes become more popular options the ability to install software on pupils' own devices will open up a raft of new questions.

- What options are there for schools to ensure that the balance between school time and personal time is not breached by monitoring of pupils on and offline activity?
- How will schools communicate the use of this technology on personal devices to pupils?
- Will the software be used to scan personal files?
- Will the software monitor activity when pupils are not in class or are not on school property?
- Will the software scan for keywords on personal messaging or when the device is offline?

Regional Breakdown

London	
Number of replies to FOI	142
Number of schools using classroom management software	101
Percentage of schools using classroom management software	71%
Amount spent	£272,063
Number of school-owned devices	39,426
Number of pupil-owned devices	0
Most popular supplier	Impero - 32
Eastern England	
Number of replies to FOI	137
Number of schools using classroom management software	99
Percentage of schools using classroom management software	72%
Amount spent	£234,219.44
Number of school-owned devices	46,093
Number of pupil-owned devices	0
Most popular supplier	Impero - 46
South East England	
Number of replies to FOI	221
Number of schools using classroom management software	144
Percentage of schools using classroom management software	65%
Amount spent	£314,986.79
Number of school-owned devices	58,529
Number of pupil-owned devices	450
Most popular supplier	Impero - 49
South West England	
Number of replies to FOI	156
Number of schools using classroom management software	102
Percentage of schools using classroom management software	65%
Amount spent	£209,861.36
Number of school-owned devices	209,861
Number of pupil-owned devices	0
Most popular supplier	Impero - 45

West Midlands	
Number of replies to FOI	177
Number of schools using classroom management software	129
Percentage of schools using classroom management software	73%
Amount spent	£294,888.07
Number of school-owned devices	294,888
Number of pupil-owned devices	0
Most popular supplier	Impero - 44

East Midlands	
Number of replies to FOI	118
Number of schools using classroom management software	97
Percentage of schools using classroom management software	82%
Amount spent	£280,551.43
Number of school-owned devices	42,008
Number of pupil-owned devices	0
Most popular supplier	Impero - 57

Yorkshire and Humberside	
Number of replies to FOI	131
Number of schools using classroom management software	98
Percentage of schools using classroom management software	75%
Amount spent	£257,128.02
Number of school-owned devices	42,676
Number of pupil-owned devices	0
Most popular supplier	Impero - 41

North West England	
Number of replies to FOI	189
Number of schools using classroom management software	128
Percentage of schools using classroom management software	68%
Amount spent	£414,068.20
Number of school-owned devices	49,615
Number of pupil-owned devices	0
Most popular supplier	Impero - 53

North East England	
Number of replies to FOI	76
Number of schools using classroom management software	54
Percentage of schools using classroom management software	71%
Amount spent	£142,568
Number of school-owned devices	22,172
Number of pupil-owned devices	965
Most popular supplier	Impero - 19
Wales	
Number of replies to FOI	73
Number of schools using classroom management software	48
Percentage of schools using classroom management software	66%
Amount spent	£100,716.72
Number of devices	14,702
Number of pupil-owned devices	1
Most popular supplier	Impero - 17
Total	
Number of replies to FOI	1420
Number of schools using classroom management software	1000
Percentage of schools using classroom management software	70%
Amount spent	£2,521,051.03
Number of school-owned devices	819,970
Number of pupil-owned devices	1,416
Most popular supplier	Impero - 403
Software - Five Most Popular Suppliers	
Impero	403
AB Tutor	160
RM Education	108
NetSupport	105
LanSchool	85

Appendix 1: Examples of Providers and the Capabilities they Offer

Provider	Screenshot	Recording of screen	Display Screen	Lock/Blank Screen	Messaging / Chat Function	Control PC	Block Internet	Internet Filtering	Internet History	Keyboard Monitoring
AB Tutor	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Acer Classroom Manager	✓	?	✓	✓	✓	?	✓	✓	?	✓
CrossTec	✓	?	✓	✓	✓	✓	?	✓	✓	✓
Impero Software	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
iTalc	✓	?	✓	✓	✓	✓	?	?	?	?
Junglebyte	?	?	✓	✓	✓	?	✓	✓	?	?
LanSchool	✓	?	✓	✓	✓	✓	✓	✓	✓	✓
Net Control ²	✓	✓	✓	✓	✓	✓	✓	✓	?	?
NetOp	?	?	✓	✓	✓	✓	✓	✓	?	?
NetSupport	?	?	✓	✓	✓	✓	✓	✓	✓	✓
RM Education	?	?	✓	✓	✓	✓	✓	✓	✓	✓
Viglen	?	?	✓	✓	?	✓	✓	✓	✓	✓

This table is not intended to be a definitive list of Classroom Management Software providers or the capabilities of the providers displayed. For more detailed information please visit the websites of each provider.

Appendix 2: Methodology

Beginning on the 17th March 2016 a Freedom of Information request was sent to all English and Welsh secondary schools which are subject to the Act.

We asked whether or not they used classroom management software, which provider that supplied the product, how much had been sent on it, how many school and pupil devices it was installed on, whether parental permission was obtained before installing on pupil devices and copies of any documentation relating to the use of the technology.

We received **1420** responses; this is equivalent to **44%**. For the purposes of this report only responses received by 9th September 2016 have been included.

Due to the sensitive nature of the data many schools asked us not to release their individual details. We are happy to respect this concern and disclose information responsibly. Accordingly, we have decided to not make the following information available:

- A full list of every school and what software they use.
- A full local authority breakdown.

This decision has been made in order to not release too much information about what measures individual schools are taking to tackle issues such as cybercrime and related problems.

Original Freedom of Information Request

Dear Sir or Madam

I am writing under the Freedom of Information Act 2000 to request information about your school's use of classroom management software, specifically I am asking the following:

1. Does your school use classroom management software? If so please specify the type of software and its capabilities.
2. How much has your school spent on this software?
3. The number of devices that the software has been installed on, please provide the following breakdown:
 - a. School-owned devices.
 - b. Pupil-owned devices.
4. Does the school obtain consent from parents before installing the software on pupil owned devices?
5. Copies of any documentation relating to the use of classroom management software in your school.

I further request that the response to Question 3 be further broken down by device type.

The Freedom of Information Act 2000 lists schools as organisations that are subject to its terms. For further information please refer to Schedule 1, Part IV "*Maintained schools and other educational institutions*": <http://www.legislation.gov.uk/ukpga/2000/36/schedule/1/part/IV> .

I understand under the Freedom of Information Act that I am entitled to a response within twenty working days. I would be grateful if you could confirm this request in writing as soon as possible.

Best wishes

Dan

Daniel Nesbitt, Research Director

Big Brother Watch

55 Tufton Street, London SW1P 3QL

Landline: 020 7340 6029| 24hr media line: 07505 448925

www.bigbrotherwatch.org.uk

About Big Brother Watch

Big Brother Watch was set up to challenge policies that threaten our privacy, our freedoms and our civil liberties, and to expose the true scale of the surveillance state.

Founded in 2009, we have produced unique research exposing the erosion of civil liberties in the UK, looking at the dramatic expansion of surveillance powers, the growth of the database state and the misuse of personal information.

We campaign to give individuals more control over their personal data, and hold to account those who fail to respect our privacy, whether private companies, government departments or local authorities.

Protecting individual privacy and defending civil liberties, Big Brother Watch is a campaign group for the digital age.

If you are a journalist and you would like to contact Big Brother Watch, including outside office hours, please call +44 (0) 7505 448925 (24hrs). You can also email press@bigbrotherwatch.org.uk for written enquiries.

Email: info@bigbrotherwatch.org.uk

Postal address:

Big Brother Watch
55 Tufton Street
London SW1P 3QL

Website:

www.bigbrotherwatch.org.uk