KEITH BRISTOW, NCA DIRECTOR GENERAL, SPEECH TO THE POLICE FOUNDATION.
JOHN HARRIS MEMORIAL LECTURE 24 JUNE 2014

POLICING BY CONSENT IN THE DIGITAL AGE

Ladies and gentlemen, good afternoon.

It is an honour to have been asked to deliver this year's John Harris Memorial lecture.

The late Lord John Harris was a man of distinction and achievement who made a vast contribution to the worlds of policing and home affairs in which many of us operate.

I feel privileged to stand here, conscious of the prestigious speakers who have stood here before me, and in front of such a distinguished audience, including of course Lady Harris.

My speech today is, fundamentally, about the law enforcement tools we need to tackle child abuse.

It is also about the fact that the capability we have to tackle this abuse, and to tackle the abusers, is being eroded significantly.

That erosion is set to get worse, and the stakes are high.

When an indecent image of a child is created, a child is abused. That child is then victimised repeatedly every time the image is shared.

And, whilst the data is not definitive, an analysis of several studies in 2011 suggested that up to 55% of people who share indecent images also abuse children directly themselves.

The NCA has an important role and voice in this debate.

We are the first agency to be given responsibility for leading the UK's fight to cut serious and organised crime.

We may have the power to direct, but this is a power we are yet to need. The levels of willing collaborative partnership across UK law enforcement today exceed anything I have experienced in my career and we are delivering tangible evidence of what we can achieve together when our collective resources are coordinated and targeted.

85% of the NCA's officers deliver or directly support operational activity.

We have an international network and hold specialist capabilities which we share with our partners – and we're investing in these to ensure we are in the best possible position to lead the UK's fight against serious and organised crime.

The NCA is in part a result of the evolution which takes place as criminal threats change and policing and law enforcement change with them.

Once, there were regional crime squads, set up in response to the increased ability of organised criminals to cross force boundaries as our road network improved.

When criminal groups began operating on an increasingly national and international basis, we had the National Crime Squad and the National Criminal Intelligence Service, and a corresponding rise in the use of intelligence techniques to tackle an increasingly resilient threat.

More recently, we had the Serious Organised Crime Agency, which created a specific focus on tackling high end criminal activity. But SOCA did not have a leadership role, and it operated in an environment where the end to end response was not always coordinated effectively.

The NCA is the next stage in a proud tradition stretching back 50 years – indeed, much further in border protection – and represents a step change in the UK's response to serious and organised crime.

When I started my law enforcement career as a police cadet in the mid 1980s, being robbed was a personal, face-to-face affair.

The crime would take place in a physical location.

It may have involved a weapon and the victim would have lost whatever they were carrying on them at the time – a watch, or a wallet for instance.

There would be an immediacy to the crime, and the victim would have had direct contact with the perpetrator.

For the criminal, making money from the robbery would also be a physical face-to-face transaction, perhaps via a 'fence', possibly in a second-hand or pawn shop, with a scrap of paper and a handful of notes changing hands

Then, as now, the nature of the crime determined the response and the investigative tactics.

This could have involved a foot chase, or a media appeal to the public for information, or house-to-house enquiries.

Footprints and fingerprints could be taken from the scene of the crime.

In some instances, police may have relied on an informant – all very Sweeney, and all very 'analogue'.

Now, new crimes have emerged alongside the traditional threats.

That face-to-face robbery has been joined in the criminal repertoire by online scams and account hacking.

Victims may be unaware that a crime has even taken place.

There may be no witnesses.

The perpetrator is unlikely to live in the victim's community. He or she could be from anywhere in the world.

The proceeds could be laundered virtually in online space

There will be no physical fingerprints to dust for or footprints to match.

So, when crimes are committed in the digital virtual world rather than the analogue physical one, our investigative tactics must be very different.

For a start, a lot of that investigation will take place in the same digital space. The trail back to the perpetrator will often be an electronic one.

We will be looking for a username – not issuing a mugshot. Typically, the perpetrator will hide their identity.

The elements of the investigation will not necessarily be contained within a single force area. It is likely we will need to contact foreign law enforcement agencies – and they will have their own processes and their own legal frameworks.

At a cyber crime conference recently a speaker asked the audience of several hundred people for a show of hands for those who had been robbed, burgled or had something stolen from their person.

A few hands went up, here and there.

The speaker then asked for a show of hands for those who had been the victim of an online scam, fraud or hacking attempt.

Dozens of hands went up.

Even this simple survey shows us how the nature of criminal threats has changed.

So there are new ways in which criminals can separate you from your money.

But these changes are also taking place in the distressing world of child abuse.

The NCA warned in its National Strategic Assessment earlier this year that the online sharing of child abuse imagery would increase, along with the online streaming, on-demand, of real-time child sexual abuse

Offenders who might have been sufficiently discouraged by the risks in the 'real world' to stop short of committing abuse in person, or accessing indecent images, now have a global environment in which they can connect with other abusers – and with victims

Some of them use digital media to blackmail their victims as part of that exploitation, which increases the potential for self harm and, in extreme cases, suicide

Offenders can have multiple victims, simultaneously, in numerous countries

The investigative tools at our disposal in the virtual world need to be just as effective as the ones we have used in the physical one.

I'm not talking only about what we think of as 'cyber crime'. There is now a digital element to nearly every investigation the NCA carries out.

Serious and organised criminals communicate electronically, just as we all do. You have a mobile in your pocket – it will email, text, phone, locate you, inform others, tweet, skype, and access Facebook.

And criminals are using their phones in exactly the same way, with one critical difference – they also use theirs to commit crime.

The public understands the traditional tools of crime fighting.

For many years they have understood mug shots, line ups, informers and pursuits.

In the 20th century we added fingerprint technology.

Even more recently, DNA and forensic analysis.

If we do our jobs professionally and with respect, and if we comply with a clear lawful and ethical regime, then on the whole the public consents to these tactics.

They know why they work, they know that they matter, and they know that without them law enforcement's ability to protect people gets substantially more difficult.

It is a trade off. We consent to CCTV on street corners because we understand how this form of intrusion on our personal privacy makes us safer.

If it did not protect us, we would not accept the intrusion.

The public has largely come with us on these tactics because they accept the trade off, and that is crucial.

Quite simply law enforcement cannot function unless the public has confidence in us.

“Policing by consent” has always been the foundation of the UK’s system of law and order. It is what distinguishes the UK as having one of the finest law enforcement systems in the world.

We are public servants. We have a contract with the public – our duty is to protect them, and we embrace this responsibility with pride.

As law enforcement officers we are given coercive powers. We have the power to arrest and detain, to deprive someone of liberty and freedom.

We have the ability to collect personal information on criminal suspects when we are investigating them.

That is a significant responsibility. It is why we must hold ourselves to the highest standards possible.

And it is particularly important given that some of the powers we hold are exercised, by their very nature, out of sight of the public.

It will become even more important.

As more of the crime threats we face migrate into a digital space - and the way we investigate them changes - it is quite possible that more law enforcement activity will become less visible to the public. This is crime which does not happen on street corners.

We owe it to people to explain the rationale for the techniques we need to employ now and in the future. And we need their consent if we are to be granted them.

When it comes to some of law enforcement’s digital investigation techniques, we have not yet explained ourselves well enough – and in my judgement we do not yet have public consent for their use.

When I speak with my friends and family about law enforcement activities in the digital world, it is clear that they are not convinced about some of the capabilities we need.

These are rational, practical, reasonable people. They are the British public. And they are not convinced.

The failing, if there is one, lies at least in part with law enforcement – but not with the people we serve.

And the space left by this failing isn’t a vacuum waiting patiently for us to fill it whenever we are ready.

It has been filled, now, already, and has been for some time - by a commentary which draws together state surveillance and Edward Snowden, and makes no distinction between the purposes of different information or the needs of different agencies.

Yes, at the root of all these things is the fundamental issue of civil liberty and the right to privacy.

To be a member of civil society means accepting that ‘absolute privacy’ may not be realistic. We cannot function as a society if we exclude others.

And when it comes to law enforcement the question is now, as it always has been: what is the trade off? Where does society permit the tipping point to sit between allowing certain intrusions because of the greater protection they afford?

The question can only be answered if we openly and honestly describe the position that we are in, without fear or favour, and without falling back on sensationalism or sentiment, and allow the public to judge.

And there is one particular law enforcement capability - one that is critical to protecting the public from serious and organised crime - on which we urgently need to describe that position and invite that judgement.

The capability is the acquisition and use of Communications Data.

As you know, Communications Data is the who, where and when of a communication – but not its content.

It tells us when communication was made, between which devices, and where the devices were– but not what was written or said.

Communications data is not interception. To the average person, communications data could seem rather two dimensional in comparison with interception

And yet communications data is often the only way to secure convictions against the most dangerous criminals, who are expert at remaining deliberately hands-off in the commission of serious crimes.

It can effectively demonstrate links between conspirators

It can disprove false alibis, and prove genuine ones.

It can also provide time-critical intelligence to stop a serious crime in action and save lives

And for all those reasons it is something on which law enforcement depends in over 90% of serious crime investigations

But despite its value, law enforcement's access to communications data has diminished, and there is a significant risk that it will continue diminishing.

The Court of Justice of the European Union has overturned the EU Data Retention Directive

The result is that the requirement in the UK for Communication Service Providers to store communications data for 12 months could also now be overturned.

It means there is a strong likelihood that UK CSPs will no longer retain Communications Data unless they have 'a business need' to do so.

Perversely, they may be compelled by law to delete records which are critical to law enforcement's ability to keep people safe

So even if we can succeed in winning the hearts and minds of the public in the case for accessing communications data, there may simply be no data to access.

The collective impact of this development, and our inability so far to produce a clear public picture of the protection that communications data provides to society, could be devastating for law enforcement's ability to disrupt serious and organised crime

I am a law enforcement officer. You would expect me to say that. So let me talk specifics.

The majority of our use of communications data is for the most serious offences – murder and attempted murder, rape, kidnap, armed robbery, and firearms offences.

I could talk to you today at length about those.

But where I really think we need to bring renewed focus is on young people – how they operate in a virtual environment, the challenges this presents for law enforcement and how communications data is increasingly important in keeping them safe.

Young people are phenomenally active online – for many it is their main mode of communication. Globally, 40% of us used the internet in 2013, but in the UK that rises to a staggering 93% of 5 to 15 year olds.

They use it to connect with their friends, to build networks, share pictures, and organise their social lives.

Feeling accepted and included by their online peers can be essential to their sense of identity.

They are often more web-savvy than teachers and parents – the very figures in their lives responsible for protecting them.

But they are also particularly vulnerable in that online space. Their activity is less guarded – and criminals know it.

The kind of protection we now need to offer young people is in my view inextricably linked to a robust communications data regime.

Historical communications data is of particular value to child sexual exploitation investigations.

Child sexual exploitation is often facilitated by the internet and can take place over many years.

Communications data is still overwhelmingly the most powerful tool available to those investigating child sexual exploitation and identifying and safeguarding its victims and potential victims.

Communications data allows investigators to capture the true extent of a criminal's offending by identifying the victims they have been in contact with; chatrooms they have accessed; who they have contacted there; and other child sexual offenders with whom they may be sharing Indecent Images of Children, or with whom they are conspiring with to sexually abuse children.

Limiting the amount of communications data CSPs can retain will prevent law enforcement from identifying and investigating child sexual offenders, identifying and disrupting the spread of Indecent Images of Children, and identifying and safeguarding victims and potential victims.

Earlier I touched upon the differences between crimes committed in the physical and virtual worlds – and how these differences impact on an investigation.

Communications data is not only of value in protecting children in cyber space. It makes a difference in tangible, physical ways

A child contacting Childline in a state of desperation after suffering bullying or abuse might do so via a computer rather than by telephone.

They might not leave a name or contact details.

If as a result of their distress a child is considered to be at risk of taking their own life, we can – and we have - used communications data to locate children quickly, before they harm themselves, and to get them the support they need.

Academic opinion is divided on the likelihood of an image offender going on to abuse children directly, but analysis of several studies in 2011 suggested that this figure is up to 55%.

The right communications data capability will allow law enforcement to identify and disrupt more of these people before they cross that horrific threshold.

Without communications data, the police would not have known that Jessica Chapman's mobile phone had been turned off in the vicinity of Ian Huntley's home.

The blackmailers linked to Daniel Perry's apparent suicide in Scotland would not have been identified.

Can you imagine, in a different era, restricting the ability of the police to talk to witnesses, secure and preserve exhibits, and search registration numbers of cars on the Police National Computer?

Every day, children are targeted by criminals and paedophiles on the internet. If we do not ensure that our investigative techniques keep pace, we are complicit in allowing their protections to be stripped away

Map across the investigative techniques we deploy in the physical world to the virtual, and we arrive at communications data.

It brings criminals to justice.

And equally importantly it can prove an individual's innocence.
Defence teams use this data to prove that someone was miles away from where a crime was committed. In some cases it can be the only evidence of that fact.

We need communications data to help prevent miscarriages of justice which are devastating to the victims of crimes, as well as those wrongly accused of committing them.

I make no apology for fighting to avoid a situation where the prosecution may not be able to prove criminal associations, conspiracies and criminal activity, and where the defence may not be able to prove alibis, identify witnesses and corroborate defences.

It is an understandable fear that communications data robs individuals of their privacy.

The question of how much privacy we want to protect as individuals, and how much we are prepared to exchange in return for other protections, has never been so important or so immediate.

That question is being asked now against a backdrop of public mistrust, and a perception that any individual could be subject to speculative scrutiny.

We cannot undo this by saying 'trust us, we will protect you'

So how do we make the distinction and rebuild an accurate understanding?

I believe there are three elements to this. The first is absolute clarity about the process by which law enforcement must abide to access anyone's data.

There is a tightly regulated regime which puts the onus on the investigator to demonstrate – and document - at the outset the clear purpose behind their request.

First, they must identify the offence which is under investigation.

No offence, no data.

Then, explain why the information is necessary.

This means showing how the person under investigation and the communications data are linked - and how both are linked to specific criminal activity.

No link, no data.

Then, explain why the communications data route is a proportionate one. The investigator must show what they expect to find, and how that will progress their investigation.

If it's disproportionate, no data.

The investigator must assess the risk that their request might uncover information which is not related to criminal activity, whether data relating to an innocent member of the public might inadvertently be obtained, and if so how it will be identified and deleted.

There are further stages of approval around feasibility, and only then will a request be considered for authorisation.

The whole process is overseen by the Interception of Communication Commissioner's office, which is completely separate to, and rigorously independent of, law enforcement, and which ensures the powers are being used correctly at all times.

Sir Anthony May, the current holder of that office, recently praised the UK for having "one of the strongest systems of democratic oversight for protecting privacy."

The reality of law enforcement's use of Communications Data is a far cry from the myth of hoovering up every phone call without justification, accountability or scrutiny.

We do not do this, but the enduring perception that we do now fundamentally damages our efforts to protect the public.

The second element in rebuilding understanding is honesty about the alternatives we would need without communications data

Collecting communications data is a far less intrusive technique than some of the other options that we would have to resort to without it, to deliver the same level of protection to the public:

More surveillance, more use of human intelligence sources, and more intercept.

None of those is an appealing prospect, for the public or for law enforcement.

Communications data allows us to investigate more crime and make better use of public resources.

It is also completely coldly factual.

The third element is judging us by what we do.

I recognise that the consent afforded to anything law enforcement does rises and falls on its ability to deliver against public expectations.

If we deliver the right outcomes – and, just as importantly, in the right way – we become relevant to the public we serve.

And if we are relevant, we are more likely to be trusted, and more likely to have the public's support.

This is the circle of policing by consent.

And this is why the onus is on all of us to make clear exactly what use we make of communication data - and the investigative and judicial outcomes which justify its use.

I hope some of the examples I have given today are a start.

Because if the public does not agree to this, then the principle of policing by consent fails.

If we risk using a power that the public will not accept, that too will inevitably fail.

I am a citizen and a family man and in those roles I want law enforcement to have the capabilities to keep us safe.

Our children are not 100% of the population but they are 100% of the future. We must nurture and protect them.

I am not talking about different sides of one coin. In balancing the every day risks each one of us has to navigate in our lives, we give up some freedoms in exchange for others.

For me, the ability for our children to roam safely in an online environment, and to be protected, is no different to wanting them to play safely in a park or socialise with their friends and to be protected.

By permitting law enforcement to access specific data – when it suspects someone of criminal behaviour, when it meets the necessity and

proportionality tests, and when it operates within a robust legislative framework – then you will have given your children greater freedom by permitting law enforcement to police that environment.

The nature of crime is changing. We need to adapt and ensure our response evolves accordingly.

We can only police by consent – and to achieve this, we must have a concerted effort from across the law enforcement world to secure public support for the approach and tools we need

For me, personal privacy and law enforcement capability are not mutually exclusive.

I believe that that through the effective, proportionate and well-regulated use of communications data we can afford people the liberty to get on with their day-to-day lives.

Perhaps the trade-off question needs to change.

Perhaps we should no longer be asking how much privacy we are prepared to sacrifice for certain protections, but rather how much protection we are prepared to give up to preserve our privacy.

What I find unthinkable is the prospect that by the time law enforcement has made its case, and had it heard, considered and – I hope - accepted by the public, our capability may have already deteriorated to the point where my officers cannot do their job, and people's lives and safety are put at risk as a result.

Knowing the risk, it is my responsibility to speak up.

Fast forward to the likely scenario if we don't act now and the public will quite rightly be demanding to know why law enforcement didn't have the foresight to influence this vital debate when it had the chance.

Thank you for your attention.