RESEARCH AND PRACTITIONERS' INSIGHT

END-TO-END ENCRYPTION:

THE (FRUITLESS?) SEARCH FOR A COMPROMISE

By Ciaran Martin

Professor of Practice in the Management of Public Organisations
Blavatnik School of Government, University of Oxford

Bingham Centre for the Rule of Law: lecture delivered at Jones Day, Tudor Street, London

November 2021

CONTENTS

INTRODUCTION

I am conditioned as a 23-year veteran of the British civil service to search for the middle ground and an elegant compromise. But occasionally, some issues arise where that is just not possible.

I have long feared that tonight's subject – end-to-end encryption – is one such topic. And in case I was tempted to temper that view, yesterday, I received, from friends, authoritative reports of forthright condemnation of my views, one each either side, of the argument I would make this evening.

This is remarkable in two ways. First, I've not spoken on the issue since leaving government as head of the National Cyber Security Centre more than a year ago. Second, at the time of receiving these messages, I hadn't finished writing these remarks, let alone shared them with anyone. At least my lack of preparation was demonstrably fair to both sides.

So I feel some real trepidation. But I am going to assume genuine good faith on both sides of the argument having dealt with both sides of it for quite a few years.

On the one hand, I absolutely do not believe that governments want to hoard everyone's data and spy at will on its own citizens and are using emotive cases as cover for that goal.

I do believe governments have genuine and well-founded concerns about how vital national security and law enforcement capabilities, and in particular, online child sex abuse.

On the other hand, I do not believe, for one second, that those who oppose governments' plans on end-to-end encryption are indifferent to those threats. In particular, I find it highly inappropriate and deeply offensive to portray those on that side of the argument as being unconcerned about the horrors of online child sex abuse.

I do believe that those who oppose governments' plans on end-to-end encryption are genuinely and deeply convinced that there is no way to address governments' concerns without weakening privacy and cyber security, possibly catastrophically.

SOME HISTORY AND CONCEPTS

It is worth reminding ourselves of the historical background here, because in my view, that, along with the technical complexity of the subject, explains why the issue is so fiendishly difficult.

There isn't the time this evening to give an authoritative account of the history of governments and encryption. As an aside, for an excellent and very accessible account, I would recommend the book Intercept The Secret History of Computers and Spies, by our host, Gordon Corera.[1]

But we can broadly summarise the history of governments and digital encryption in four phases.

The first, up until about the 1970s, has encryption as essentially the exclusive preserve of governments. The need for identical keys and massive computing power, combined with the economic and computing structures of the age, mean that cryptography is the stuff of the secret state, of the Enigma heroes, the early NSA and GCHQ, their Cold War adversaries, and no one else.

The second phase starts with the discovery and popularisation of public key cryptography in the 1970s. The era where two young West Coast academics – Whit Diffie and Marty Hellman – make mainstream commercial application of encryption possible, having reached – eventually, after a very tense stand-off – some sort of accommodation with the NSA. This is a revolution in cryptography and an essential foundation for the digital age. We now know, of course, that Britain's GCHQ knew about the breakthrough several years earlier, but did not disclose it: a sure sign of the tension between state and expert when it comes to encryption.

The third phase is the period between the horrors of 9/11 in 2001 and the Snowden leaks of twelve years later. Digital communications have become ubiquitous and the bad guys use them too: not just terrorists, but money launderers and paedophiles too. Governments improve their capabilities accordingly, particularly prompted by the urgency of international terrorism. But despite public key cryptography and other developments, cyberspace is fundamentally insecure; application of encryption is patchy. Some of it is implemented weakly, and carelessly, and even when done well, in some cases the government can compel its covert disclosure by law. The result is what some called the 'Golden Age of sigint'; signals intelligence; the use of bulk data collection and analysis to counter threats and harm.

The fourth phase, in which we're still living, is the aftermath of this 'Golden Age'. Societies and their governments have become more worried about digital insecurity. Improvements are made: they make users a bit safer but sometimes make the job of governments in detecting badness online a bit harder. And then Edward Snowden's leaks turbocharge the process.

Two things happen technically, amidst a backdrop of a sharp deterioration in trust between governments on the one hand and the tech industry and security and privacy advocates on the other. First, the strong encryption of datasets held by communications service providers is applied ubiquitously. And the large scale roll-out of end-to-end encryption of messaging platforms takes off. As a result, governments begin to warn grimly of 'going dark' in the face of serious online threats.

[1] Intercept: The Secret History of Computers and Spies, by Gordon Corera, Weidenfield and Nicholson, 2015

SOME HISTORY AND CONCEPTS

To understand why, we should return to the very basics of lawful intercept, as introduced in this country by Oliver Cromwell when he established the General Post Office in 1657 (though spying on communications long predates that). This allowed for the warranted opening of any letter: indeed most historians take the view that Cromwell's motivation in setting up the system was to strengthen the security capabilities of the Commonwealth rather than upgrade its communications infrastructure.

Now let's consider how such intercept can be done in a postal context. A very good place to look is a sorting office. You're searching for letters to a known wrong'un, so you give his name to the head of the sorting office and show your warrant. That is the basic principle by which lawful intercept has worked down the years, whatever the changes in communications technology.

Under ubiquitous encryption, the problem is that the sorting office is in America. But, at least in theory, the state can seek to cut a deal with the US government for regulated access (as the UK has done with the Cloud Act agreement with the US).

But under end-to-end encryption, the problem is there is, as some would see it, there is no sorting office at all (or at least there are far too many micro-sorting offices to make the old concepts any use). As such, it is a much more existential threat to the centuries old model of lawful intercept.

THE INDUSTRY SIDE, AND WHY IS THIS ALL ABOUT FACEBOOK?

That is, of course, how things looked from the perspective of governments.

How did it look to the tech industry?

It must be remembered that the introduction of end-to-end encryption was both logical and, in consumer terms, very, very popular. Apple has always made a big deal of it. So did WhatsApp, now part of Facebook, now Meta. Services like Telegram and, most strikingly, Signal came along: Signal explicitly on a not-for-profit, end-to-end encryption model that has proved wildly popular.

The laggard has been Facebook, excepting WhatsApp. And this has led to the weird and distorting situation that so much of the recent debate has been about this one company.

In a blogpost on April 30 of this year, Gail Kent, who is with us this evening, said that the rest of Facebook's services were on their way to being end-to-end encrypted, but not until the end of 2022 at the earliest[2].

Concern about this is deeply felt. In the UK, the National Society for the Prevention of Cruelty to Children pointed out in a 2019 report that around half of the reports of online child abuse came from Facebook platforms.[3] The figure for the United States in terms of reports to the National Center for Missing and Exploited Children is more than 90 per cent: in 2018 that amounted to some 16.8 million referrals[4].

These startling and concerning figures are presumably why Five Eyes Interior Ministers when they wrote an open letter to Mark Zuckerberg in October 2019, imploring him not to introduce end-to-end encryption.

But surely, the only reasonable interpretation of these figures is not that Facebook's platforms account for the vast majority of online child sexual abuse. That is not a credible assertion. It is simply because Facebook have not yet implemented end-to-end encryption.

The difficult reality is that these policy interventions are, in effect, demanding that one very large and increasingly unpopular company does not do what most of its competitors have already done.

Of all the legitimate complaints we can have about Facebook's business practices, catching up with the rest of the industry on what has become broadly accepted as best-practice in messaging platform security is surely not top of the list.

Why has it become industry standard? The essence of the end-to-end encryption argument – to maintain the sorting office analogy – is there must be no infrastructure, no sorting office, so no one at all can get it because there's nothing to get into. If something does exist, then there is no way of restricting access to it by governments alone. As Susan Landau of Tufts University pithily puts it, "if we build it, they will break in". If the UK and US governments can come in, so too, potentially, can the criminals, the North Koreans, the Russian state and so on.

It is therefore entirely understandable that most cyber security experts strongly support end-to-end encryption. If cyber security were the sole objective of government technology policy, end-to-end encryption would enjoy unqualified Government support. It is the potential for its misuse in serious crime and national security threats that leads to the present dilemma.

Let us now look at how the UK government has approached that dilemma.

[2] Messenger Policy Workshop: Future of Private Messaging, blogpost by Gail Kent, Messenger Policy Director, 20 April 2021, at https://about.fb.com/news/2021/04/messenger-policy-workshop-future-of-private-messaging

[3] Private Messaging and the Rollout of End-to-End Encryption: The Implications for Child Protection, page 4. Published by the National Society for the Prevention of Cruelty to Children on 26 January 2021, at https://www.nspcc.org.uk/globalassets/documents/news/nspcc-discussion-paper-private-messaging-and-the-roll-out-on-end-to-end-encryption.pdf

[4] Open Letter to Mark Zuckerberg, from Rt. Hon. Priti Patel MP, Home Secretary of the United Kingdom, William P. Barr, Attorney General, United States of America, Kevin McAleenan, Secretary of Homeland Security (Acting), United States of America, and Hon. Peter Dutton, Minister of Home Affairs, Australia, 4 October 2019, at https://www.gov.uk/government/publications/open-letter-to-mark-zuckerberg/open-letter-from-the-home-secretary-alongside-us-attorney-general-barr-secretary-of-homeland-security-acting-mcaleenan-and-australian-minister-f

THE POLITICS AND POLICYMAKING OF END-TO-END ENCRYPTION

Analysis of the government's approach needs to distinguish between its tone and its substance. The tone is often forthright and technically wrong: think of David Cameron's garbled remarks in January 2015 which implied he wanted a ban on encryption. The policy substance is more subtle.

The Investigatory Powers Act, passed later that year, secures, in the words of the Home Office, the power to "require a communications service provider to help the Government deal with the encryption they apply to data". This takes the form of a "Technical Capability Notice". A TCN can require a company "to maintain the capability either to remove encryption or to provide data or communications in an intelligible form"[5].

The substance of how the UK intends to implement that legislative position is more constructive than it's often given credit for by critics.

In a remarkable and my view positive intervention – tonally and substantively – at the end of 2018 in a blogpost for the Lawfare website, Ian Levy, the NCSC's technical director, and Crispin Robinson, from the intelligence side of GCHQ, set out principles for an informed debate on exceptional access to encrypted material[6]. (I should declare an interest at this point as a member of the board of the organisation where both authors worked, and the line manager of one of them. All of these remarks are, however, my own and I have not consulted anyone in government about them).

To my mind, that blog is unfairly remembered in some circles because of one specific suggestion of what became known as the 'ghost protocol'; a suggestion that hidden law enforcement or intelligence users could be added to exchanges exceptionally after due, warranted process.

More important is the overall approach, which remains the core of UK policy. The key message of the blog was, to quote its first line, "in…cyber security, details matter".

If, they argued, the end-to-end encryption debate is conducted in abstract principle, then we will get nowhere. However, if we look at the details of how the technology actually works, then something might be possible which satisfies both sides. The 'ghost protocol' was only an idea for discussion in that context, not a prescribed solution. The blog was intended to launch the search for solutions.

Sadly, at least in the public domain, much of the intervening three years at ministerial level seem to have been spent shouting at Facebook. But British policy does, however, appear to have returned to this position by way of an intervention by the Home Secretary in early September in an article for The Daily Telegraph.[7]

[5] Written testimony of the Home Office to the Judiciary Committee of the United States Senate on the matter of Encryption and Lawful Access, Evaluating Benefits and Risks to Public Safety and Privacy, 10 December 2019, at https://www.gov.uk/government/publications/open-letter-to-mark-zuckerberg/written-testimony-of-chloe-squires-director-national-security-home-office

[6] Principles for a more informed exceptional access debate: blogpost by Ian Levy, Technical Director of the National Cyber Security Centre, GCHQ, and Crispin Robinson, director for cryptanalysis, GCHQ, for Lawfare, 29 November, 2018 at https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate

[7] "I call on the world's tech giants: please don't put profit before safety", by Rt. Hon. Priti Patel MP, Home Secretary, Daily Telegraph, 8 September, 2021 at https://www.telegraph.co.uk/politics/2021/09/08/priti-patel-call-worlds-tech-giants-please-dont-put-profit-safety/

THE POLITICS AND POLICYMAKING OF END-TO-END ENCRYPTION

Here, yet again, the divergence between tone and substance cannot be ignored. The first sentence of the news article accompanying the Home Secretary's piece read:

> "Priti Patel has launched a worldwide hunt for tech wizards to crack Facebook's encryption so Britons are protected from child abusers and terrorists".[8]

Everything that is objectionable about the government's tone is summed up in that one, quite obviously politically briefed sentence. In fact, the actual policy the Home Secretary was announcing was completely different, and rooted in the Lawfare article approach. The government was in fact announcing something called a Safety Tech Challenge. It offers a research prize of £85,000 to up to five groups to develop:

> "innovative technologies which demonstrate how tech companies could continue to detect images or videos showing sexual abuse of children while ensuring end to end encryption is not compromised".[9]

[8] "Priti Patel seeks encryption crackers to keep children safe on Facebook": News report in the Daily Telegraph, 8 September 2021 at https://www.telegraph.co.uk/news/2021/09/08/priti-patel-seeks-encryption-crackers-keep-children-safe-facebook/

[9] See https://www.safetytechnetwork.org.uk/innovation-challenges/safety-tech-challenge-fund

THE SEARCH FOR A COMPROMISE

This is the best, most balanced statement of UK policy objectives I can find. And, in the spirit of good faith, let us accept it for what it is: a genuine attempt to find a compromise that protects end-to-end encryption.

But let us also accept that it is technological “cakeism”. In a government headed by a Prime Minister famous for the phrase that he is pro-cake and pro-eating it, this is saying we can have both targeted access and well-functioning end-to-end encryption.

And as with all arguments about cakeism, the question is whether it is really possible.

There are reasons to approach this question with humility and scepticism. If it was easy, it would have been done by now.

Several extensively researched proposals have failed, thus far, to convince sceptics, and not just the so-called ‘ghost protocol’. Another idea is known as ‘quorum key escrow’, where very tightly controlled keys are held. This idea invariably founders on the existence of a key at all, and the potential, however well-guarded, for its compromise.

The closest we have so far come to an attempt by one of the major players is Apple’s announcement earlier this year of a plan to introduce what is called ‘client-side scanning’ onto their devices. This does not break the end-to-end encryption cryptographically. But it does open a door between the device and the provider, which can be used without the device owner’s knowledge to detect and report potentially harmful content.

Apple have now suspended the introduction of client side scanning and a range of cryptographic experts have lined up against it. I will not go into the technical objections: the paper most worth reading is called Bugs in our pockets: the risks of client side scanning[10] which, among its stellar cast of authors includes the aforementioned Whit Diffie and Susan Landau as well as Bruce Schneier and Ross Anderson. But one easy-to-understand objection is, yet again, if responsible democratic governments can use this capability for the purposes of countering child abuse, so too can authoritarian and adversarial states for a variety of other, less noble purposes.

The overall point here is that we do not yet appear close to a technical solution that could allow us to have our lawful access “cake” and “eat” our end-to-end encryption feast.

And, frankly, if someone can develop the innovative technology the Home Office plan envisages, he or she is likely to be worth a lot more than the £85,000 promised by Her Majesty’s Treasury.

The government has some way to go to convince people that it has not just launched a competition to develop the digital age equivalent of alchemy.

[10] Bugs in our pockets: the risks of client side scanning: by Hal Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Jon Callas, Whitfield Diffie, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Vanessa Teague, Carmela Troncoso. Pubished by Cornell University, 14 October 2021, at https://arxiv.org/abs/2110.07450

THE SEARCH FOR A COMPROMISE

And this leads to the point about how it is decided if a compromise is possible.

One of the legitimate points about those concerned about end-to-end encryption is the fact that decisions which could affect huge swathes of intelligence and law enforcement capability is decided by the governing committees of gigantic American companies rather than national democratic legislatures. I have no answer to that, other than to say it cannot be dealt with other than as part of the wider debate about the power of Big Tech.

But let me, instead, turn the argument on its head for the purposes of the encryption debate.

The government is, in effect, demanding that the tech industry does something to keep access open (at the same time, of course, as demanding the highest possible levels of cyber security).

The industry, backed by most of the relevant expertise, is saying that what the government is demanding is simply not possible.

Some experts say, in effect, that the government is arguing not against a policy decision, but against mathematics.

The government's response is simply to assert that no, you are wrong, it is possible, and you should go away and do it.

Surely though, the onus is on the government, not the industry, to set out clearly and transparently how they believe these two seemingly irreconcilable objectives can be met in the same regulatory package?

As 2022 approaches, surely there are better ways to spend the time than ordering Facebook not to emulate the rest of the industry. Instead, surely they should set out detailed technical options for scrutiny and debate about how the two objectives can co-exist across technology as a whole, and try to win support for them?

If they think, for example, client-side scanning is a workable model, why not publish a detailed technical paper to contest the narrative in Bugs in our pockets and see if sufficient people are swayed by the argument?

I passionately hope that this effort to have the best of both worlds works, and I wish the government well in its attempts. But we have to contemplate a situation where it doesn't.

At that point, two things are of paramount importance from whichever side of the debate prevails. One is honesty. The other is generosity
of spirit.

If it is to be the case that end-to-end encryption poses such a threat to public safety that its implementation and use must be constrained by law, then governments need to be absolutely open about what that means.

It means levelling with the public that however hard we will try, and we will try hard, digital protections are not as good as they might otherwise be, but that the greater good demands it. That is a legitimate policy choice.

But as well as honesty, transparency is needed. There should be more openness, for example, and where possible, about what sort of Technical Capability Notices are needed, why, and how they are applied. If we learned anything from Snowden, it's that the state needs to seek informed consent for what they do in this space. Relying on a general sense of 'those with nothing to hide have nothing to fear' is a terrible idea.

PERSONAL VIEW

By now, you will probably have realised that this is not the outcome I would favour. With a heavy heart, given my sympathy with intelligence and law enforcement challenges and long association with many of them as colleagues and friends, I cannot see how we, as a free, open and increasingly digitally dependent society, would gain from such a decision.

My personal position is this: if a suitable technical compromise solution that commands widespread industry and expert confidence cannot be reached, then security must win, and end-to-end encryption must continue and expand, legally unfettered, for the betterment of our digital homeland.

I say this for three reasons.

First, there is the inexorable reality of technological developments. End-to-end encryption exists, it works, and it makes sense. Tech companies know it and privacy campaigners know it. But so too do citizens.

And, frankly, so too do policymakers.

I won't embarrass individuals by getting out my phone and listing all the senior people I know involved in this issue, in multiple jurisdictions and professions, who are stored in my Signal contacts. These friends and colleagues are acting rationally, not hypocritically: their important work can, sometimes, be better protected in this way. That's why this revolution in digital security cannot, Canute-like, be wished away, anymore than public key cryptography could be held back indefinitely.

It is hard to see a blanket ban on end-to-end encrypted services, and it hard to see an increasingly security- and privacy-savvy population doing anything other than flock to them, the bad minority as well as the good majority. That is our new, permanent reality, whatever Facebook decides to do and whatever governments decide to do about Facebook.

Second, given this reality, I believe that whilst the consequences for law enforcement and, to a lesser extent intelligence, are real, they can be mitigated, perhaps significantly so.

Let me dwell on this for a moment. Just as at the start of this talk I said I had no time for those who portrayed the privacy and cyber security side of the arguments as indifferent to the horrors of child abuse, I similarly have no time for those on that side of the argument who accuse their opponents of 'playing the child abuse card'. (I particularly recoil at the social media memes where opponents of government policy post 'think of the children' memes.) The difficulties for law enforcement in particular posed by end-to-end encryption are real, they have been for some time, and that will continue.

I have no doubt, given the figures quoted earlier, that should Facebook move to end-to-end encryption as planned it will cause genuine difficulties for law enforcement: we must be honest about that. But it's surely wrong to portray this as some sort of evil or wilful move by the company. It's the completion of what the rest of the industry has already done; the final phase in the latest stage in a decades old cat-and-mouse situation where technology changes, criminals use the new technology, the good guys catch up, the technology changes, and the cycle starts again.

Looked at this way, end-to-end encryption is just another practical operational issue, not an issue of principle.

Frankly, even in the immediate aftermath of Snowden, it was not really true that governments 'went dark', they 'went spotty': they had access to lots of data, but not all of the data they needed to see, or had access to before.

To draw on the language of the UK government's Lawfare blog, details matter. There are many different options for the good guys to prevent and detect serious crime in the age of end-to-end encryption. iMessage has been end-to-end encrypted for years but we now know that billions of messages have been stored in the cloud; Apple are changing this and another subset of cat-and-mouse begins.

Perhaps the best way of illustrating this point is the FBI's attempts to unlock the iPhone of the San Bernardino terrorist murderer in 2015. This is not, I accept, a question of end-to-end encryption. It was about, as you will recall, the fact that the phone of the terrorist was in the possession of the authorities, but could not be unlocked. So the FBI (using a statute from 1789) sought to compel Apple to write some code to unlock the extremely well protected phone (to give a sense of the extent of the protection, there was a famous case of a woman whose toddler had taken her phone and made so many attempts to log in, the message was she could try again – in 47 years).

Apple refused, stating the obvious point that if it created a way into iPhones for the FBI in this one case, it created a way into iPhones everywhere, for everyone, which did not currently exist. The application was denied and appealed. But the appeal was dropped, because the FBI managed to access the phone in a different way.

In other words, there was another way. There isn't always another way. But there often is.

And overall, would it really have been better if, even in this extreme, unusual and difficult case, the US government had won and compelled Apple to do something that would potentially compromise all of its phones?

This leads me to my final reason.

It is a now national and international imperative that our increasingly digital societies are increasingly digitally secure. Post pandemic, when we all went to live and work online in our artificially created digital environment, cyber security is a public good. In societies like ours, it is increasingly hard to think of instances where the benefit of weakening digital security outweighs the benefits of keeping the broad majority of the population as safe as possible online as often as possible. There is nothing to be gained in doing anything that will undermine user trust in their own privacy and security.

But that is not to say that these decisions come without desperately difficult downsides.

That is where generosity of spirit, and a realisation of the genuine problems of those in intelligence and law enforcement trying to keep us al safe, must come in. Instead of traducing the good intentions and vital work of policing and intelligence with offensive accusations that they're 'playing the child abuse card', why not redouble efforts to help bring offenders to heel in the new technological dispensation?

So perhaps it's best to leave the last word to Marty Hellman, victor of that epochal struggle between cryptographic revolutionaries and democratic states in the 1970s. Of his encounters with the secret state, he recalled, many years on: "My view back then was that they [the National Security Agency of the United States] were not interested in national security. They were interested in job security. Now I look at it very differently. I do think they were concerned. They did have some legitimate concerns, and I should have taken those into account. I still would have taken the position that I did, but I would have fought it more fairly".[11]

Fight it more fairly. Wise words as we build the safer digital societies of the future.

[11] Corera, Intercept, pages 109-10

www.bsg.ox.ac.uk

@blavatnikschool

linkedin.com/school/blavatnik-school-of-government