The Federal Bureau of Investigation v. Apple Inc.
A United Kingdom Perspective
by Dr. Brian Bandey
Foreword

The recent battles between the giants of Apple Inc. and the Federal Bureau of Investigation in the US have been heard around the world. International commentary on them has covered issues of worldwide interest – from articles on the security of the Internet and the mechanisms of trust built into it; to treatises on state power verses the individual’s right to privacy.

I have been commissioned by Venafi Inc. to conduct an exercise of technical legal research to provide a UK Law perspective and analysis of these events; and thus generate a clear understanding of how our legal system would have handled the competing interests of Apple and the FBI.

In doing so, my attention was drawn to, arguably, one of the most important pieces of legislation UK Law has ever seen – the Regulation of Investigatory Powers Act 2000. The Regulation of Investigatory Powers Act 2000 is commonly referred to as “RIPA” – phonetically: ripər, rlpfər or ripə.

And as I injected the facts of FBI v. Apple into the UK legal system and began my application of RIPA – I began to think of an older ripər - ‘Jack’. The “Ripper” that stalked the Victorian streets of the East End of London. He (if it was a he) was de facto invisible and he tore through the personal rights of his prey without a thought. All fell before him.

Perhaps we have a new Jack in town – but in this 21st Century: “Jack the RIPA.”

I do mean to be amusing – but I have not found this research task funny. Quite the opposite. For it revealed a jurisprudential gulf between the legal systems of the US and the UK that has, I believe, implications that go far beyond one single industry sector but touches every business that uses IT security and relies on cybersecurity in particular. I think that might be every business?

The economic resources of the FBI dwarves that of any police force. Yet to prise the information it sought from Apple Inc., it must go before a Judge – a member of the US Judiciary properly separated from the power of the Executive. And there, in Open Court, on the record publicly available, the FBI must plead its case.

I would hear any officer, director or manager of any UK corporation say “Quite Right Too!” and “Of Course!”

Indeed, what could be more natural in a democracy for Apple management to appeal direct to its customers and the world at large.

After all, how could it be otherwise?

At law school, students are taught that the theory, letter and principles of the law sometimes find voice in practice in a very different fashion. For many people – an unanticipated and surprising fashion.

Our Jack (the RIPA) is full of surprises.
The UK, unlike the US, does not require judicial oversight to grant the type of information the FBI sought from Apple.

**RIPA Section 49 Notice:**

Lets middle-ranking police officers serve an order on a company director, officer or manager to disclose this type of information - without any judicial interference.

**Secrecy:** Recipients of a s.49 order can be obligated to keep the order a secret to all but their lawyers.

**Criminal Offense:**

Noncompliance is punishable by fines and/or imprisonment.

The legal framework and procedures to which the FBI must subordinate itself are underpinned by the concept of judicial overview and the Constitution of the United States of America itself. That’s why Jack doesn’t live there – that’s why he lives here.

Jack gives middle-ranking police officers the legal capacity to serve an order on a company director, officer or manager to disclose the very type of information the FBI sought from Apple. All without any interference from any Judge. That type of order is legally created in s.49 of RIPA and has come to be known as a "Section 49 Notice”.

And Jack can do more. The s.49 Notice can include an obligation on the notified to keep it secret that they’re the subject of the Notice and to keep it secret what the Notice is about.

Not to comply with a s.49 Notice is a criminal offence – punishable with fines and/or imprisonment. Sure – they can tell their lawyer. There are statutory defences. There are rules the police must follow in making their decision. They can appeal to a tribunal and can, a little later, take the matter before a Judge.

But, in my certain opinion, there is an uneasy truth that lies behind the letter of this law. How does Jack, how can Jack behave in real corporate life?

You see, when Tim Cook and his board began to take their decisions with respect to opposing the FBI – what was the landscape in which they worked? They could go public – they had time to make an application to the Court – they could discuss it amongst themselves – they could take advice from third parties who were not lawyers. All was “in the light”.

But with Jack: all is “in the dark”. The decision-making of a UK corporation in the UK shoes of Apple takes place in a completely different landscape. Whatever one might think of the probability of later imprisonment or fine – they will take their decisions in the context of possible arrest and criminal prosecution. The UK board is called upon to take a chance and weigh personal odds that were unknown to Apple officers.

The police don’t serve the s.49 Notice on the corporation – they serve it on officers and employees personally.

And not only that – the s.49 Notice can come with Jack’s speciality; and that is s.54 of RIPA. No “Tipping-Off”. Once again on pain of imprisonment and/or fine the director or manager can be compelled to keep the fact of being served a s.49 Notice and the contents of it a secret [but for their lawyer]. They can’t tell their wife, husband, partner, sister, brother or any other person who might support them. They can’t tell the marketing director nor the PR Agency. No – not even other board members not associated with complying with the Notice. Shareholders and stakeholders may remain perpetually ignorant of the disclosures being made. Jack doesn’t care about any of that.
US v. UK
Unlike the UK, US companies do not have to abide by an order of secrecy or weigh the possibility of criminal prosecution on the officers or employees.

FBI v. Apple is the first battle in a long war. In the UK, we must understand how RIPA impacts this battle.

Let us make no bones about it. Police officers who are well-motivated, intent on acquiring evidence that they see as critical, and determined are to be reckoned with. Especially for the senior manager who might never even had a speeding ticket in their youth.

What are the chances of conviction? Slight? Who knows? And even if they are and it became to be seen as some form of mistake – it would still mean arrest, bail applications, fingerprint processing, criminal lawyers who know Jack and the wonderful waiting rooms of the Crown and Magistrates Courts.

FBI v. Apple isn’t over. It has not now become irrelevant. Rather it is but the first battle in what I believe will be a long war. It is emblematic, an archetype if you will, of a pressure felt by law enforcement agencies around the world. A pressure to force disclosure of the inner mechanisms of cybersecurity and cybertrust.

We need to understand Jack the RIPA. Understand what he can and cannot do. But above all recognise and admit to ourselves that he exists for us in a way that he never would for Apple.

I certainly hope this briefing paper goes some small way in bringing about such corporate realisation.
**Introduction**

The facts of the two actions in the US between the FBI and Apple are well known and have been commented upon and rehearsed around the world. But the core legal principles in play between the FBI and Apple are not transferable to legal jurisdictions such as the United Kingdom.

To illustrate that legal ‘fact’ the ostensible pervasiveness of the US Legal System will be examined in the context of the Laws of the United Kingdom. In other words, if Apple was a UK Company and the Police wanted the same as the FBI – what would happen? Would the results be the same or different? And importantly – would the legal landscape in which the contest over access to cryptographic keys, digital certificates and encryption methodologies be the same?

An assumption of this Briefing Paper is that the legal landscape, over which the battle for access to the cryptographic protection in respect of an Apple iPhone 5C, is critical to understanding the matters of principle that are in play: principles of Privacy, Freedom, Judicial Overview and the Power of the State. In its legal battle with Apple, it seems that the power that the State was seeking to exercise was not overwhelming nor a given. If it was, then the FBI would not have looked elsewhere for a technology-based solution to its problem. In a sense then, it is argued that the FBI v. Apple cases are viewed by the world at large through the prism of US Legal Procedure. In this Briefing Paper we will, instead, view it through the prism of United Kingdom Law and, especially, United Kingdom Legislation.

Finally in this Introduction, please bear in mind that only some Law can be parsed. The action of the Regulation of Investigatory Powers Act 2000 is not without complexity. Accordingly some aspects of its operation, even though relevant, will not be discussed.

**What the FBI Wanted**

The FBI wanted to use Apple’s cryptographic key to sign and authorise software that would then disable security on a specified iPhone 5C.

**What the FBI Said They Needed and Why**

The detail of the Order sought by the FBI need not be repeated here. But the FBI’s wish list was [paraphrasing]:

- The FBI wanted Apple to create code - which the document refers to as a Software Image File or “SIF” - that it can load into the iPhone’s RAM without modifying any of the data already stored on the flash memory, including “the iOS on the actual phone, the user data partition or system partition.”

- The FBI wanted the SIF to be coded with “a unique identifier of the phone so that the SIF would only load and execute on the SUBJECT DEVICE.”

Essentially, the FBI wanted to use Apple’s cryptographic key to sign and authorise the SIF and then disable security on the device in question. Speculation arose that it was the intention of the FBI to gain a tool through which it could defeat the security on Apple devices in general.
The position of Tim Cook, the CEO of Apple Inc., can be summarised from press releases and reports: "In the wrong hands, this software – which does not exist today – would have the potential to unlock any iPhone in someone’s physical possession." "And while the government may argue that its use would be limited to this case, there is no way to guarantee such control." and "The FBI may use different words to describe this tool, but make no mistake: Building a version of iOS that bypasses security in this way would undeniably create a backdoor."

What the FBI Had to Do to Get It

In 1994, Congress passed the Communications Assistance for Law Enforcement Act ("CALEA"). CALEA’s purpose was to enable law enforcement agencies to conduct electronic surveillance by requiring that telecommunications carriers and manufacturers design their equipment to ensure that they have built-in surveillance capabilities. On the face of it – one might think that CALEA presented the route for the FBI to meet its needs.

But CALEA presented a number of challenges to the FBI’s position and provided no real route to the FBI in gaining the type of access they wanted in the California case. Indeed, the FBI rehearsed its ‘CALEA argument’ before Magistrate Judge James Orenstein when the FBI sought a functionally identical order against Apple in the US District Court, Eastern District of New York.

If Not CALEA – Then the All Writs Act

The closing passages of Magistrate Judge Orenstein’s decision illustrates the commonality in the FBI’s position from East to West Coast and demonstrates how the US Constitution and the power and authority of the US judiciary provided an unscaleable obstacle to the FBI:

"The government seeks an order requiring Apple, Inc. ("Apple") to bypass the passcode security on an Apple device. It asserts that such an order will assist in the execution of a search warrant previously issued by this court, and that the All Writs Act.... empowers the court to grant such relief. .... I conclude that under the circumstances of this case, the government has failed to establish either that the AWA permits the relief it seeks or that, even if such an order is authorized, the discretionary factors I must consider weigh in favor of granting the motion. More specifically, the established rules for interpreting a statute’s text constrain me to reject the government’s interpretation that the AWA empowers a court to grant any relief not outright prohibited by law."

As in all US litigation, the Constitution looms large over the proceedings and informs every action of the Law in the United States. I suggest we begin to see how the very structure of US Law checks the power of the state and balances it against the rights and needs of Apple.
It is absolutely critical to bear in mind that the legal actions between Apple and the FBI arise within the context of US Law and US Civil Procedure. Their actions, the arguments advanced and the responses of the parties and the judges adjudicating are all creatures of one, particular, complex legal jurisdiction. Legal concepts that exist in the US (and which are therefore discussed around the world – especially in the context of the FBI – Apple debacle) may not, indeed often do not, exist anywhere else in the world. They are exclusively creatures of US jurisprudence. Let us now turn our attention to another jurisdiction – the UK.

How Would the United Kingdom Law Enforcement Authorities Fare?

It was argued above that the FBI v. Apple cases are viewed by the world at large through the prism of US Legal Procedure. The first thing that becomes apparent as it is viewed through the prism of United Kingdom Law (and, especially, United Kingdom Legislation) is:

- the absence of a written constitution that subordinates legislation to it;
- the removal of judicial powers of oversight and review by specific legislation that would (ordinarily) be overturned in the US;
- the lawfulness of Parliament’s supremacy in excluding the Courts of Law from the arena of surveillance by government bodies in the absence of a written constitution that subordinates legislation to it;


In order to evaluate how UK Law would operate, a worked-example will be constructed similar to the case before the US District Court for the Central District of California.

Although the choice made here for the purposes of analysis is to juxtapose a fictional UK technology company against Apple; one could have chosen any corporation from any industry that designed or used encryption technology, cryptographic keys and digital certification.

The facts of the hypothetical case are as follows:1

---

1 The ‘scenario’ is formulated in the form of an exam question that might be put to a law undergraduate. The facts have been made somewhat banal so as to examine the law that is in action; but not trivialise the import of the subject matter of the FBI v Apple actions nor belittle the terrible losses associated with them.
The Initial Facts

Gooseberry Ltd. ("Gooseberry") is the designer and manufacturer of the smartphone called the gPhone. It runs their "Goose-OS" operating system which includes an encryption system.

- Danny Diamond is a career criminal specialising in the theft of diamonds. Mr. Diamond not only steals diamonds himself, he sells his techniques and draws up plans for organised diamond thieves around the world.

- Mr. Diamond plans and then conducts (with his 'crew') a diamond-heist. On leaving the heist, Mr. Diamond and his crew enter into a high speed car chase with the Metropolitan Police. Unfortunately, Mr. Diamond's car crashes and he is killed. His 'crew' have no information as to Mr. Diamonds inside sources for the robbery nor his contacts across European diamond robbers. That information was kept in Mr. Diamond's gPhone which was recovered – but locked – in Mr. Diamond’s getaway car.

The Law Available to the Metropolitan Police

Part III of RIPA provides a statutory framework that enables public authorities to require protected electronic information which they have obtained lawfully (or are likely to obtain lawfully) be put into an intelligible form; and to acquire the means to gain access to protected information and to acquire the means to put protected information into an intelligible form. Failure to comply with a disclosure requirement or a secrecy requirement is a criminal offence. The subject of the Section 49 Notice (as it’s called) commits an offence if they do not comply with the Notice. The prison sentences that apply are: (i) up to 5 years imprisonment in respect of a case involving National Security; and (ii) up to 2 years imprisonment in other cases.

It should also be borne in mind that it is possible for a Section 49 Notice to require the subject of it to keep the fact of the serving of this notice a secret. So under Section 54(4) RIPA ("Tipping Off") a person who makes a disclosure to any other person of anything that he is required by a section 49 notice to keep secret will be guilty of an offence and liable: (a) on conviction by a Crown Court, to imprisonment for a term not exceeding five years or to a fine, or to both; (b) on conviction by a Magistrates Court, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum, or to both.

So not only can a UK citizen be compelled (on pain of fine and/or imprisonment) to provide the passwords and all other information necessary to unlock their private data (including, for example, cryptographic keys and the digital certificates used for encryption and authentication); they can also be compelled [similarly on pain of fine and/or imprisonment] to keep it a secret that it’s happening to them.

Included within a s.49 Notice can be a demand for supporting information which takes the form of proprietary software that will render intelligible otherwise unintelligible data or more complex material such as algorithms for either or both encryption and decryption of data. That is,
in law, unlikely to be a “Key” per se. But under RIPA such electronic data may, nonetheless, be relevant to such data. As such, any reference to a key or to key material can include supporting information. Thus where supporting information is in the possession of the person subject to the s.49 Notice, and where supporting information is in the possession of a person, a notice for the disclosure of a key may require the disclosure of such supporting information.

The Section 49 Notice and Corporations

Living individuals only can be imprisoned – corporations cannot. Accordingly, s.49 Notices are served on the officers or employees of a corporation. The Police will first look to serve on a senior officer. In this context ‘senior officer’ means a director, manager, secretary or other similar officer of the corporate body (and where the body is managed by its members a director means one of its members).

The FBI v Apple Scenario Under UK Law – More Facts and Applying the Law

With the Law in mind now – let us return to the “Danny Diamond Case” – elaborate the final set of facts and apply the Law. Here we will then view the FBI v. Apple case through the glass of RIPA.

The Police have Danny Diamond’s gPhone in their possession. It is locked and they do not have the technical means to defeat the security protocols of Goose-OS and believe (indeed have good reason to believe) it contains information revealing the diamond theft and smuggling organisations of Europe.

Accordingly the Police approach the Directors of Gooseberry. They require the following of Gooseberry: (i) the Key to unlock the gPhone in question; or (if not possible); (ii) the Goose-OS algorithms that will permit the Police to interrogate the gPhone without wiping any of the data in it; or (iii) the Goose-OS source code so that the Police can cause a 3rd party to write a computer program that will interrogate the gPhone without wiping any of the data in it; and (iv) the Goose-OS algorithms and Source Code relevant to the manner in which the gPhone locks for a period of time so that the Police can defeat it and gain access to it as quickly as possible.

The Directors refuse to provide the information. They claim it is their most sensitive proprietary information and intellectual property. Furthermore it creates a backdoor or enables the creation of a backdoor that will open any gPhone to any government agency.

A Police Superintendent authorises the issue and service of a s.49 Notice on the CEO, CTO and Principal Product Architect requiring them to disclose the above data. In addition, the s.49 Notice contains a notice under RIPA that prevents “Tipping-Off” (to be discussed below). Thus effectively, all of the preceding persons must keep it a secret that a s.49 Notice has been served on them.
Applying the Law

It is correct to say that the Police Superintendent must take a number of statutory factors into account when deciding if a s.49 Notice should be served. It is also correct to say that complaint may be made to the Investigatory Powers Tribunal and applications to the Courts may be made.

But, and this is a very big ‘but’, a middle-ranking police officer is exercising a statutory power to compel a person to deliver up highly sensitive, secret and valuable information (including intellectual property) without any judicial oversight at the time when the order is made.

Note also that such Superintendent can cause the persons who have been served with the s.49 Notices to keep that service and the contents of the Notice secret. The Law allows them to tell their lawyers – but they cannot tell the press, nor make a press statement nor tell their spouse, partners or friends. They are, de facto, alone and isolated. They are alone and isolated in the manner in which they would not be if they had been arrested on a criminal charge for a crime that carried a custodial sentence and were being kept in a police cell. In such a circumstance they would, at least, have the right to contact a spouse or partner and thereby promulgate the fact that they had been charged.

In the FBI v. Apple case, Timothy Cook was able to use Apple’s press agencies and the media to give the public notice of the actions being taken against Apple and to advertise Apple’s position in respect of the application by the authorities to the Court (in itself – a public act).

This could not take place under RIPA.

The directors and managers would begin their compliance with the s.49 Notices [possibly] straightaway – in secret. It is accurate to say defences could be made as to the burdensomeness of the obligation and lawyers could be instructed straightaway [even if a corporate lawyer could be found on a Saturday morning]. But those officers and managers, if they chose to refuse to comply with the s.49 Notice there and then, would be gambling with their liberty. Not so – never so – for Tim Cook and his team.

And it was never so for Tim Cook and his team because Apple is subject to US Law. But the fictional Gooseberry is subject to UK Law and therefore subject to RIPA.
Conclusions and Observations

It is suggested that there is one overwhelming and inexorable conclusion that must be drawn when viewing the factual matrix of the FBI v. Apple cases through the prism of United Kingdom Law – and that is nothing would be the same in the United Kingdom.

As a matter of Law, it would not have been necessary for the Police to make an application to a Judge for an Order to compel Apple ("Gooseberry") to make it’s disclosures. Indeed, the opportunity for Apple to make its own applications to the Court on the immediate issue of disclosure are not a given under RIPA. Just as importantly, those company officers served with s.49 Notices must make an almost instant decision [depending on the pressure being put upon them by the Police and especially if the Police see the matter as having aspects touching on National Security] as to whether they are to cooperate or not.

It is suggested that this is a matter of paramount importance – the officers of Apple were placed in an environment where, if a decision to not comply with a Court Order was made; that 'contempt'; could be argued before the Court later. Not so in the United Kingdom where RIPA is in play. The decision takes place in the context of arrest. A context of being charged with a criminal offence and being taken to a Police Station and interviewed there.

The company officers involved will be gambling, no matter what legal counsel will be available to them, with their liberty. They will be gambling with the effect on them and their family if charged with a criminal offence and then prosecuted. And finally on the matter of this wagering [with high stakes], the company officers and managers involved may not be able to tell anyone (other than their lawyer) – not their wife, husband, partner, mother, father, brother, sister or any other person concerned with or dependent upon their well-being. In a determined Police action using s.49 and s.53 of RIPA to the full, it is hard to see how any corporation could react on an immediate basis and oppose the Police action.

In closing then, the corporate world of the UK should not imagine, for one moment, that the procedures of the US District Courts are in anyway applicable to them.

Nor should the UK corporate world imagine that the action of RIPA is confined to technology companies. It is of universal relevance and applicable to any enterprise making or using encryption technologies, keys or certificates.

It is this one important, indeed singular area for all enterprises where the “Corporate Veil” simply does not exist. Corporate Officers and Managers are exposed directly to the criminal law provisions of RIPA.