RIGHT TO PRIVACY AND LAW ENFORCEMENT

TEXT OF A LECTURE PRESENTED AT THE OGUN STATE JUDGES’CONFERENCE (OJSC), 27TH SEPTEMBER 2016

BY

PROFESSOR ADEDEJI ADEKUNLE
DIRECTOR-GENERAL,
NIGERIAN INSTITUTE OF ADVANCED LEGAL STUDIES (NIALS)
Digital communications afforded by the internet, mobile smartphones and Wi-Fi enabled devices, have become part of everyday life.

In this digital era, communications technologies have also enhanced the capacity of governments, enterprises and individuals to conduct surveillance, intercept and collate data.
This phenomenon rightly raises concern about unwarranted intrusion into the right of privacy of individuals, companies and other entities.

It is the duty of the law to bring to harmony the conflicting interests of the individual with those of an increasingly complex society.

It is also the duty of the judiciary as an appropriate body to determine whether a law transgresses the implicit limits of privacy.
A. Insight into the concept of privacy and the enforcement of public order and safety

B. Jurisprudence from Canada, the United States and the United Kingdom relating to electronic surveillance/wire tapping and data protection

C. Nigerian judiciary’s approach to the concept of the right of privacy

D. Recommendations for the Nigerian judiciary
WHAT IS PRIVACY?

An essential human need at the core of our democratic values.

‘a claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others’ (Westin 1970)

‘the value of privacy must be determined on the basis of its importance to society, not in terms of individual rights….. (Solove 2009)
Whilst it may be difficult to develop a single comprehensive definition of privacy, overall the term can be viewed, not only as a personal value intrinsically beneficial to preserving our sense of self, but also an essential value for society.

For the purpose of this discourse, I regard law enforcement in the broad sense of the application of law in civil and criminal spheres.
The United Nations General Assembly (UNGA) recognises that international human rights law provides the universal framework against which any interference in individual privacy rights must be assessed.

The Universal Declaration of Human Rights (UDHR) 1948 sets out the terms for protection of privacy –

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.
The right to privacy does not feature at all under the African Charter on Human and Peoples’ Rights (ACHPR) 1981.

Section 8 (1) of the European Convention for the Protection of Human Rights and Fundamental Freedoms 1950 provides that ‘everyone has the right to respect for his private and family life, his home and his correspondence.’
The only basis for such interference by a public authority will be under the following conditions:

- if it is necessary in a democratic society;
- it is in the interest of national security, public safety or economic wellbeing of the country;
- for the prevention of disorder or crime;
- for the protection of health of morals;
- for protection of the rights and freedoms of others - s. 8 (2)
Gradually, the right to privacy has become universally recognised as a fundamental right due to its inclusion in the most important international and regional human rights treaties.

Some aspect of the right to privacy is incorporated into almost every constitution in the world and into the general laws and jurisprudence of those countries without written constitutions.

Countries that have no written constitutions extend privacy protections through their other legal norms such as procedural rules, evidentiary codes and statutory protections, or fuse such right to privacy protection with data protection (which interprets privacy in terms of management of personal information).
Protection can be facilitated at the national level by privacy legislation incorporating one or more of the following parameters:

- Information privacy, which involves the establishment of rules governing the collection and handling of personal data such as credit information and medical records;
- Bodily privacy which concerns the protection of people’s physical selves against invasive procedures such as drug testing and cavity searches;
- Privacy of communications, which covers the security and privacy of mail, telephones, email and other forms of communication; and
- Territorial privacy, which concerns the setting of limits on intrusion into the domestic and other environments such as households, the workplace or public space.
The extent to which these parameters are provided for in legislation and its interpretation by the courts in Nigeria are examined in this paper.

The questions which are addressed subsequently include:

a) to what extent is the constitutional right to privacy enforceable? and

b) what litmus test should the judiciary utilise in determining when a right to privacy has been invaded in the Nigerian context and within the ambit of the 1999 constitution?
The basis for right to privacy laws in Nigeria is section 37 of the 1999 Constitution. It provides that:

- the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected.

This provision encompasses the privacy of the person (i.e. from unwarranted incursions into physical, emotional and personal attributes); the sanctity of homes and property (i.e. from unauthorised searches or trespasses); and the protection of correspondence and conversations from being intercepted or diverted.
The right to privacy under the 1999 Constitution is not an absolute right because section 45 of the same Constitution provides for circumstances that permit derogations from that right.

Section 45 provides –

Nothing in section 37...shall invalidate any law that is reasonably justifiable in a democratic society –

(a) in the interest of defence, public safety, public order, public morality or public health; or

(b) for the purpose of protecting the rights and freedoms of other persons.
The implications of this section are such that where existing or new legislation relating to health, environment, criminal justice administration, town planning, etc. infringes an individual’s right to privacy, the courts are faced with determining the constitutionality of the law in light of the provisions of section 45.

Specifically, the court must consider the following elements:

- Was the legislation in question a reasonable one?
- Is it justifiable?
- Is such legislation necessary and does it presently suit the democratic society in Nigeria?
- Is such a legislation in the interest of defence, public safety, public order, public morality or public health? Is such legislation necessary to protect the rights and freedoms of other persons?
I advance the following preliminary views based on section 45:

- Any kind of invasion of privacy that is not backed by law is unconstitutional;
- It is for the court and not the person enforcing a law to determine whether that law is firstly reasonably justifiable under a constitutional democracy, and secondly, whether it is made in the interest and for any of the purposes outlined under section 45;
- Where the limitation measures proposed by the legislature are considered excessive in relation to the interests protected, the court will pronounce the law unconstitutional;
- In terms of procedural law, it should matter to the courts how law enforcement officers procure evidence or methods used by the state to investigate infractions of the law, because where breaches of privacy are not checked or discouraged, the state apparatus becomes unduly oppressive – and that cannot be good for any democratic society.
JUDICIAL DECISIONS ON RIGHT TO PRIVACY IN NIGERIA

The combined cases of Shugaba v Minister of Internal Affairs, (1998) Ajayi v AG Federation (1992) and Abiola v Abacha (1998) clearly establish that damages can be awarded for breach of fundamental human rights like the right to privacy.

With regards to unauthorised search and seizure, the following cases Mallam Abdullahi Hassan & Ors v EFCC & Ors (2013); Commandant-General, the Nigeria Security and Civil Defence Corps & Anor v Emmanson Ukpeye (2010); Federal Republic of Nigeria v Joseph Daniel (2011) reveal that the courts are not willing to go beyond the ambit of section 45 in this regard.

They are strict in insisting that any such law that authorises search and seizure must be ‘reasonably justifiable’ and in the interest of either public order, safety, morality or health.
Whatever may be the justification to construe derogations of constitutional rights liberally, one might suppose that where a breach exists, the court should adopt a strict enforcement approach to the right to privacy, particularly where an erosion of privacy leads to the procurement of some material that can be used in evidence.

Paradoxically, the Nigerian courts have stuck to the very unsatisfactory principle in Sadau v State, that the illegality attending the procurement of relevant evidence has no bearing to its admissibility. This case relied on the Privy Council (PC) decision of Kuruma v R which pronounced the position of the law as follows:

- The test to be applied in considering whether evidence is admissible is whether it is relevant to the matters in issue. If it is admissible...the court is not concerned with how the evidence was obtained.
Information Technology (IT) is being deployed increasingly in major sectors – aviation, power, financial, security, health and educational systems. IT has enhanced productivity and cut costs in these sectors, but has also increased risks to attacks that are not limited by boundaries or territory.

With the aid of biometrics, internet and GPS digital footprints or signposts are created with transactions on the computer or a mobile telephone. Financial transactions, air tickets, consumer purchases readily yield detailed personal information about persons with the aid of sophisticated tracking and hacking devices.

While the benefits of IT are unquantifiable, the risk that personal data will be compromised is also high. Various concerns have therefore been expressed regarding the lack of protection under any Nigerian legislation for citizens whose personal data (biometric) is collected and stored for the purpose of National ID Cards, National Driver’s License, etc.

Whilst other countries like the UK have relevant legislation to guide the use and sharing of such data information, Nigeria currently has no specific, comprehensive data privacy or protection legislation in place.
The 2015 Cybercrime (Prohibition, Prevention etc.) Act criminalises unlawful interception of non-public data. The penalty is a maximum of 2 years imprisonment and 5 million naira fine (section 12).

The Act does not mention the word ‘privacy,’ but it provides for the retention and protection of data in computer based system by financial institutions and criminalises the interception of electronic communications in financial institutions (Section 16).

It appears that the inclusion of this provision was a direct acknowledgement of current possibilities of electronic interceptions by hackers or outside forces in electronic communications and transactions.
A Data Protection Bill 2015 is currently before the House of Representatives.

The Bill relates to collection of and protection of personal information or data and makes provisions for a Privacy Commissioner to address violations under the provisions of the proposed legislation. Unfortunately, there are no specific references to electronic surveillance of privacy rights contained therein.

It is not expected that such legislation, even when enacted, will radically affect breaches of digital privacy where stipulated, by provisions of statute, and in pursuit of measures proportionate to the level of mischief sought to be prevented.
The Terrorism Prevention Act (TPA) 2013 provides for instances when interception of communication will be allowed.

This can only be achieved through the judicial process.

The TPA empowers a judge upon an \textit{ex parte} application to grant an interception of communication order. The order allows for such intrusive measures such as requiring the service provider to intercept and retain a specified communication, authorize relevant law enforcement agency to enter any premises to install devices and execute covert operations. Section 29(1)TPA.

In my respectful view, the moderation by the judicial arm as distinct by arbitrary rationalisations by the enforcement agency is a crucial indicia of a limitation that is reasonably justifiable in a democratic society.
Section 148 of the Nigerian Communications Commission (NCC) Act 2003 provides that the Commission may unilaterally order that any communication or class of communications to or from any licensee, person or the general public, relating to any specified subject shall not be communicated or shall be intercepted or detained, or that any such communication or its records shall be disclosed to an authorised officer mentioned in the order cannot for this reason be justified.

The validity of such intrusion would have been tested in Nigeria if Mr Rickey Tarfa, SAN had not quite inexplicably withdrawn a suit he had instituted against one of the service providers alleging unauthorized intrusion into his private telephone records.
There are two draft bills pending before the National Assembly regarding interception of private communications in Nigeria: the **Interception and Monitoring Bill 2009** and the **Telecommunications Facilities (Lawful Interception of Information) Bill 2010**.

Both bills also fall short of the requirement that the necessity for the interception or the curtailment of the right to privacy should be moderated by the court.

The purpose of the first bill is to ‘provide for the interception and monitoring of certain communications, to provide for the interception of postal article and communications and for the monitoring of communications in the case of a serious offence or if the security or other compelling national interest is threatened, to prohibit the provision of certain telecommunication services which do not have the capacity to be monitored and to regulate authorised telecommunications monitoring.’
There are also laws that are sensitive to the right to privacy. An example of such a law is the Freedom of Information (FOI) Act 2011.

This Act obliges public institutions to disclose records in their custody upon request, permits the public institution to deny an application for any information which constitutes an invasion of personal privacy. (Section 12 (1) (a) (v), FOI Act 2011).

However, it is disheartening to note that the FOI Act only makes provision for the protection of personal information in the custody of public agencies and institutions within the meaning of the Freedom of Information Act.

There is no provision for the protection of personal information in the custody of private organisations or non-governmental organisations. For example, financial service firms such as banks, insurance companies, brokers, and other private organisations that process personal data.
The immediate consequence of this gap in Nigerian law is the absence of an institutional framework and weak remedial structure.

The 21st century - the digital age - has moved beyond skeletal constitutional provisions to protect citizens from abuse of technology. This leads me to put forward some posers:

- Without a strong protective framework, what hope does the citizen have against the coercive apparatus of the state?
- What protective measures can the Nigerian state deploy when law enforcement agencies intrude on privacy of citizens beyond the Fundamental Human Right (FHR) enforcement action?
- What measures are deployed to ensure that when courts act on evidence thus procured, impunity is not being promoted? Is the criminal justice system improved by condoning such invasions?

I examine the approach by three jurisdictions: Canada, the United States of America (US) and the United Kingdom (UK) in resolving these questions and I draw lessons for Nigerian judiciary from their experience.
There is no explicit constitutional right to privacy in Canada.

Section 1 (a) of the Canadian Bill of Rights guarantees ‘the right of the individual to life, liberty, security of the person and enjoyment of property and the right not to be deprived thereof except by due process of law.’

The Canadian Charter of Rights and Freedoms also contains a similar provision to that contained in the Bill of Rights, but does not confer a right to privacy.
The Privacy Act 1983, Canada’s first major privacy legislation was adopted to regulate the collection, use and disclosure of personal information by public or government bodies. It imposes obligations on over 250 federal government departments and agencies to respect privacy rights, explaining how federally regulated bodies can collect, use and disclose citizen’s personal information, and the process by which such citizens may request to access and update such information.

The second legislation is the Personal Information Protection and Electronic Documents Act (PIPEDA) 2000 and it entered into force on January 1, 2004. PIPEDA regulates the private sector and it seeks to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in the course of commercial transactions in the private sector.

PIPEDA is modelled on the Canadian Standards Association (CSA)’s Model Code for the Protection of Personal Information. It contains ten noteworthy privacy principles which are included in PIPEDA – accountability; identifying purposes for which information is collected; consent; limiting collection; limiting use, disclosure and retention; accuracy; safeguards; openness; individual access; challenging compliance.
The Privacy Commissioner oversees compliance with both legislations, with the Federal Court of Canada in charge of enforcing PIPEDA by ordering companies to comply with the Act, publish notices or corrections, and award damages, including punitive damage.

Despite the uniqueness of PIPEDA, Scholars like Davison have also acknowledged that the most invasive of Canada’s privacy is that of electronic surveillance.

He notes that the authorities now have the ability to secretly intercept and record all types of phone conversations (land-line and cellular); text messages, emails and virtually every other form of electronic and wireless communication.

In order to conduct electronic surveillance of communications in Canada, the police must obtain prior authorization from a judge by providing sworn evidence demonstrating the belief that an offence has taken place and that the interception of private communications may lead to the obtaining of information about that crime. Unless one of the parties to the communication has consented to its interception, additional requirements also apply to wiretap orders.
Freedoms are read carefully against the backdrop of the exclusionary rule contained in section 24 (2) of the same Charter.

Section 8 provides that ‘everyone has the right to be secure against unreasonable search and seizure.’

Section 24 (1) empowers anyone whose rights and freedoms have been infringed under the Charter to apply to a court of competent jurisdiction to obtain remedies.

By virtue of section 24(2), where a court concludes that evidence was obtained in a manner that infringed or denied any such rights in (1), such evidence shall be excluded if it is established that the admission of same in the proceedings would bring the administration of justice into disrepute.

In R v Tessling (2004), the Supreme Court of Canada spoke of the need for vigilance in protecting the integrity of personal information in an age of expanded means for snooping. It therefore held that the evidence admitted could be included against the defendant, and allowed the appeal.
In *R v Plant* (1993), the court held that even though the police check of computerized records was not unreasonable, it could not be concluded that the accused held a reasonable expectation of privacy in relation to the computerized electricity records which outweighed the state interest in enforcing the laws relating to narcotics offences. Hence, the evidence obtained against the accused could not be excluded as the ‘admission of real evidence does not tend to bring the administration of justice into disrepute.’

In *R v Grant* (2009), the court reasoned that the purpose of Section 24(2) is to maintain the good repute of the administration of justice. It noted that The court’s role is to balance the assessments under each of these lines of inquiry to determine whether, considering all the circumstances, admission of the evidence would bring the administration of justice into disrepute.
In the case of *R v Duarte* (1990), the Supreme Court of Canada agreed that, with regards to wiretap/audio surveillance technologies, the law should assume that individuals continue to have a reasonable expectation that their private conversations will not be recorded by state agents.

In *R v Tse* (2012) and *R v Rogers Communications* (2016), the Supreme Court ruled that the failure of authorities to provide after-the-fact notice to targets of wiretaps, done without warrant, violated s. 8 of the Charter, noting in the latter case that telecom companies have the obligation to protect the privacy of their subscriber’s personal information, and that police must make sure that requests for this information are minimally intrusive.

In *R v Spencer* (2014), the police obtained Internet Service Provider (ISP) subscriber information associated with an IP address without prior judicial authorization. Upon appeal, the Supreme Court of Canada decided that (i) Canadians have a reasonable expectation of privacy in their use of the Internet; (ii) a police investigation does not, in and of itself, constitute ‘lawful authority’ to obtain personal information without a warrant; and (iii) a police request to an ISP to voluntarily disclose customer information constitutes a ‘search’ under the Charter.
There is no explicit privacy provision included in the US Constitution nor is there any comprehensive statutory basis for asserting such a right.

Citizens’ privacy in the United States is somewhat protected by statutes such as the Privacy Act of 1974 and the Freedom of Information Act. Such statutes adopt a sectoral approach to this issue.

The Fourth Amendment of the US Constitution protects the ‘right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures.’ This exclusionary rule requires that evidence obtained as a result of official lawlessness be excluded in court. This rule was established by the US Supreme Court in *Mapp v Ohio*.

The US Supreme court held that all illegally obtained evidence in searches and seizures is inadmissible into court at the federal and state levels.

Consequently, in *Herring v United States*, the issue was whether the exclusionary rule should apply when the police conducted an illegal search in reliance on a record-keeping error made by another police employee. The court held that the rule did not apply because the error did not rise to the sufficient level of culpability.
The United Kingdom does not have a written constitution that enshrines a right to privacy for individuals and there is no common law that provides for a general right to privacy.

However, the UK has incorporated the European Convention on Human Rights into its national law, which provides for a limited right of respect towards an individual’s privacy and family life.

The primary legislation in the United Kingdom (UK) which regulates the holding of an individual’s personal data by companies, and consequently has an impact on information concerning the private lives of individual is the Data Protection Act (DPA) 1998.

It entered into force in 2000.
The DPA contains eight principles which regulate how personal data should be handled:

i) personal data shall be processed fairly and lawfully;

ii) personal data shall be obtained only for one or more specified and lawful purpose;

iii) personal data shall be adequate, relevant and not excessive;

iv) personal data shall be accurate and updated;

v) personal data shall not be kept longer than is absolutely necessary;

vi) personal data shall be processed in accordance with rights of data subjects under the Act;

vii) personal data must be kept safe and secure; and

viii) personal data must not be transferred outside the European Economic Area without adequate protection.
The Information Commissioner’s Office (ICO) regulates the DPA 1998.

Although breaching the data protection principles alone is not a criminal offense, it may give rise to claims for compensation from data subjects that have suffered damage and distress, or the imposition of a financial penalty from the ICO.
In November 2015, the UK government presented to Parliament an Investigatory Powers Bill. The Bill is meant to consolidate UK laws governing surveillance and to replace the Data Protection and Investigatory Powers Act 2014, which is set to expire on December 31, 2016.

The Bill seeks to preserve current blanket data retention requirements for communications data and add a new requirement for communications service providers to retain users’ ‘Internet connection records’ for up to 12 months.

The Bill would make explicit the legal authority for intelligence and security agencies, the police, and the armed forces to hack into computers, networks, and mobile phones (“equipment interference”), on both a targeted and bulk basis. Although a judge would have to approve warrants for hacking, the targets could be broadly defined even under targeted interference warrants.

The government has been criticized for using the Bill to legitimize mass surveillance, as the Bill represents a ‘threat to the privacy of millions of people in the UK and abroad, setting a dangerous example for other governments.’
The English common law rule is such that all relevant evidence is admissible.

There is no rule that evidence obtained illegally or in breach of the European Convention on Human Rights is inadmissible, but ‘the court may refuse to allow evidence on which the prosecution proposes to rely to be given if it appears to the court that, having regard to all the circumstances, including the circumstances in which the evidence was obtained, the admission of the evidence would have such an adverse effect on the fairness of the proceedings that the court ought not to admit it.’ (Police and Criminal Evidence Act 1984, s. 78).
The European Court of Human Rights has sought to interpret the extent to which Article 8 of the European Convention on Human Rights ensures right to privacy from secret surveillance activities.

The Court in Klass and others v Germany (1978) established that Article 8 is only able to deploy its full protection capacity if the mere existence of legislation or secret measures is considered an interference.

The Court opted for this approach, bearing in mind that the ‘mere existence of the legislation’ generated a ‘menace of surveillance’ which necessarily affects the liberty of interaction between users of communication services and hence, presents an ‘interference’ by a public authority with the right to respect for private life and correspondence.

In Malone v the United Kingdom (1984), the court held that the existence of legislation that allowed the interception of phone calls amounted to infringement on the applicants’ rights.

Similarly, in Liberty and others v the UK (2008), the court extended its position to general programs of surveillance as well as targeted wiretapping of private conversations.
However, the traditional depiction of the British approach to privacy is challenged by the enactment of the Human Rights Act (HRA) 1998 which imported the protections of the European Convention on Human Rights (ECHR) into domestic law including Article 8 which provides that ‘everyone has the right to respect for his private and family life, his home and his correspondence.’

The Act requires legislation to be read and given effect in a way which is compatible with the rights under the ECHR as far as it is possible to do so, and prohibits public authorities from acting in a way which is incompatible with a Convention right.

This provision serves to put a check on state officials who may want to rely on existing legislation to justify arbitrary extension of power granted by such legislation in search and seize operations.
The above discourse on the three jurisdictions reveal that Canada and England are focused on trying to achieve a balance between upholding the fundamental right to privacy and ensuring the fair administration of justice by disallowing illegally obtained evidence.

On the other hand, the US judiciary focuses on evidentiary exclusion on the basis of deliberate, reckless or grossly negligent violation of a fundamental right to privacy to serve as a deterrent.

It appears that the judiciary in Canada and the United Kingdom are committed to utilising privacy legislation to enforce the right to privacy, providing redress for victims whose privacy has been invaded in any manner.
Hence, the judiciary in these jurisdictions have been able to use judicial precedents and a commitment towards ensuring the proper administration of justice to uphold the right to privacy, thus giving little or no room for state officials to engage in arbitrary use of the powers granted by search and seize legislation.

The judiciary in these jurisdictions, particularly Canada and the United Kingdom, is able to achieve these through existing legislation which provide a remedy against such exercise of power by state officials who may be in breach of an individual’s privacy.
The importance that the right to privacy has for individuals is evidenced in the manner in which the right continues to expand and evolve to adapt to society’s needs.

The legal definition as well as the contours of what the individual right to privacy encompasses continues to develop as society advances and as technology provides new ways in which individual privacy is affected.

The advent of new technologies capable of easily infringing our private affairs has forced us to recognise the pressing need to establish with clarity what level of protection we can expect from governments with respect to our right to privacy.
It appears that Solove’s theory that 'the value of privacy must be determined on the basis of its importance to society, not in terms of individual rights' is representative of the approach of the Nigerian courts.

The single thread which runs through right to privacy claims in Nigeria is the judiciary’s objective to maintain a balance between private and public interest.

as highlighted above, the courts in Canada and the UK apply a balancing test in making evidentiary decisions with the courts considering a host of factors in determining whether admission of illegally obtained evidence would adversely affect the fairness of the proceedings or bring the administration of justice into disrepute.

The US applies its exclusionary rule in order to achieve deterrence of state officials from behaving recklessly in the exercise of their duties and to ensure that the right to privacy among other fundamental rights is not invaded.
The Nigerian judiciary has no ‘crutch’ on which to hinge its arm except by the express provisions of sections 37 and 45 of the 1999 Constitution.

The ultimate solution to this quandary is the need for an urgent review of privacy laws in Nigeria.

It appears that our laws are somewhat lagging behind in terms of protection of the right to privacy. Content and framework prescribed in the bills before the National Assembly (NASS) obviously need to be improved upon to incorporate international best practices.
My review of the privacy laws in Canada and the UK reveal the following crucial considerations:

- Consent of subject of information or record to public disclosure;
- Establishment of protocols for exceptional disclosure or access in the public interest;
- Penalisation of wrongful disclosure;
- Institutional protection and administration of scheme of protection, etc.
It may be that a review of the bills warrants an inclusion of the ten classifications envisaged by Canada’s CSA Model Code, now incorporated in PIPEDA, and the eight principles relating to personal data as contained in the UK’s DPA 1998.

The adoption of these privacy principles, particularly the PIPEDA principles of accountability; limited use, disclosure and collection; and openness is exactly what the Nigerian judiciary obviously needs, in the light of the intrusiveness of modern surveillance methods, to review the uncritical application of the rule in Kuruma, which in any case is no longer fully representative of the law in the UK.
I suggest that the Nigerian courts toe the line of its Canadian and UK counterparts by addressing right to privacy claims from a balanced societal and individualistic standpoint, while also drawing lessons from the United States judiciary.

As interpretation of the law requires flexibility to meet with changing nature of our present democratic society, so too should the courts be able to determine the difference between excesses of law enforcement based on existing sectoral legislation and the need for the privacy of an individual to be respected.

If left unchecked, there may be a tendency for law enforcement to begin to infringe on other fundamental human rights of individuals, apart from the right of privacy.
The Nigerian judiciary must remain vigilant and prepared to uphold the right to privacy of individuals based on circumstances before it, and based on the proposed laws on privacy envisaged by NASS.
THANK YOU