

A background image showing a group of business professionals in a meeting. A man in a suit and tie is on the left, gesturing with his hand. A woman in a dark blazer is in the center, looking at a smartphone. Another person is on the right, partially visible. There are coffee cups and a tablet with a chart on the table.

CHANGING PARADIGMS, ELECTRONIC RESEARCH METHODS AND CONSENTING: ETHICAL AND LEGAL ISSUES AND HOW TO ENGAGE RESEARCH COMMUNITIES

Dr. Adrian Jjuuko

School of Law, Makerere University

Former chairperson and member TASO Research Ethics Committee

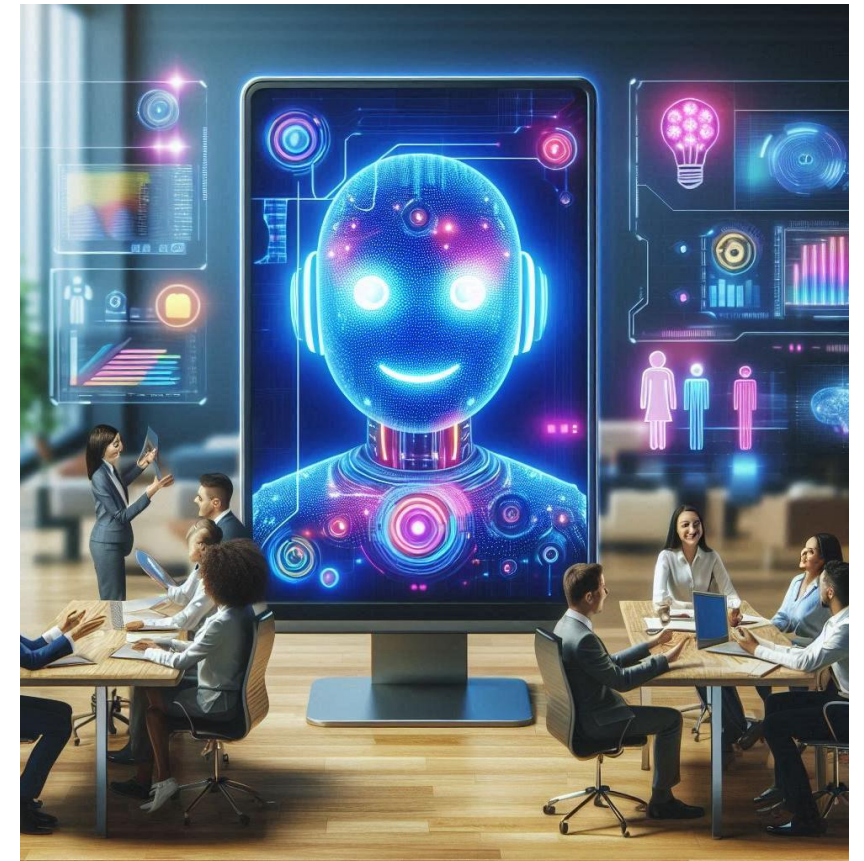
Presentation at the 12th Annual Research Ethics Conference, 2025

Hotel Africana, 21st – 22nd October 2025

22nd October 2025

CHANGING TIMES – CHANGING PARADIGMS

- We live in the computer age – the age of the internet, the age of Artificial Intelligence and the Age of the internet of things.
- Computers are now handheld and mobile.
- We can speak to people from anywhere on the globe.
- Pandemics like COVID-19 led to an exponential rise in the use of the internet and indeed in many countries the internet and digital technologies remained the only legal ways of engagement.
- The internet and electronic transactions are generally faster, cheaper and ‘cooler.’
- These developments cannot affect every other facet of our lives without affecting research. Researchers have adopted electronic research methods. However, this challenges research ethics as we know it and pose a number of ethic issues.



WHAT ARE ELECTRONIC RESEARCH METHODS?

- Electronic research methods refer to the ‘emerging range of methods which use the internet to support the creation of primary research data’. - *Claire Hewson ‘Ethics Issues in Digital Methods Research’ in Snee, H., Hine, C., Morey, Y., Roberts, S. & Watson, H. (2015). Digital Methods for Social Science: An Interdisciplinary Guide to Research Innovation. Palgrave, Macmillan, 206.*
- They are variously referred to as online research methods, web based research methods, digital research methods, e-research, and *internet-mediated research* (IMR).
- They refer to two distinct research practices – the collection of internet based data using algorithms (including now – AI) which does not involve seeking informed consent, and the conversion of offline research methods to online research methods, which usually obtains seeking informed consent. A study can also have both online and offline engagements. For example some people may be interviewed online and other physically or some data collected online and others physically.
- Our discussion today will focus on both aspects since internet based research involves access to databases such as Google and engaging research participants online.

THE LEGALITY OF ELECTRONIC RESEARCH METHODS

- Ugandan law does not prohibit electronic research – and what the law does not prohibit – it allows.
- Article 29(1)(b) of the Constitution of the Republic of Uganda, 1995 protects ‘freedom of thought, conscience and belief which shall include academic freedom in institutions of learning.’ Therefore, research is covered under this right – including electronic research.
- The Electronic Transactions Act Cap 99 has one of its objects at to ‘enable and facilitate electronic communication and transactions.’ This clearly indicates that Ugandan law recognises electronic transactions.

The legality of electronic research methods

- Under section 2, electronic transactions are defined to mean ‘the exchange of information or data, the sale or purchase of goods or services, between businesses, households, individuals, governments, and other public or private organizations, conducted over computer-mediated networks.’
- This clearly includes electronic research.
- The Uganda National Council for Science and Technology’s in its National Guidelines for Conduct of Research During Coronavirus Disease 2019 (COVID-19) Pandemic, 2020, authorised the use of ‘electronic methods for seeking, confirming and documenting informed consent in research studies.’

THE ETHICAL ISSUES PRESENTED BY ELECTRONIC RESEARCH METHODS

The key ethical concerns that arise from the use of electronic research methods are:

1. How to distinguish between public and private data
2. Informed consent related issues
 - i) How to identify the person who has actually consented and who has not since the other party is not there physically
 - ii) How to ensure that there is no third party alteration of data during transmission
 - iii) How to ensure the identify of the person presumed to be consenting in the age of AI and deepfakes
3. How to protect confidentiality of participants during electronic research – computer misuse
4. Access to computers/internet as an inclusion/exclusion criteria
5. Compensation of research participants using digital means
6. How to undertake community engagement online especially with communities that have no or limited access to internet/mobile phones

PRIVATE VS PUBLIC DATA

- Section 11(1) of the Data Protection and Privacy Act requires that a person collects personal data directly from the data subject.
- “Personal data” is defined as information about a person from which the person can be identified, that is recorded in any form and includes data that relates to the nationality, age or marital status of the person; the educational level, or occupation of the person; an identification number, symbol or other particulars assigned to a person; identity data; or other information which is in the possession of, or is likely to come into the possession of the controller and includes an expression of opinion about the individual.
- This implies that one should not obtain a person’s personal data from third parties.
- However, under section 11(2), personal data can be collected from third party sources in certain circumstances, the ones which are relevant to online research being - where the data is contained in a public record – and this includes the internet; or where the data subject has deliberately made the data public; or where the data subject has consented to the collection of the information from another source.

Private vs Public data

- This part of the law makes a distinction between private personal data and public personal data.
- Collection of 'private' personal data over the internet requires consent while 'public' private data that is already available on the internet does not.
- However, even in the case of public personal data,' care must still be taken to ensure that accuracy of the data and this may sometimes require seeking the clarification of the data subject.

THE INFORMED CONSENT PROCESS IN ELECTRONIC RESEARCH

- In terms of the law, Article 41 of the Constitution of the Republic of Uganda, 1995 (as amended) provides for the right of access to information held by the state or its organs. This however means that no one has a right to access information that belongs to private individuals or companies or organisations.
- Article 27(2) of the Constitution protects the privacy of persons – including research participants.
- The Data Protection and Privacy Act Cap 97 regulates the collection and processing of personal data. Section 7(1) provides that a person shall not collect or process personal data without the prior consent of the data subject.
- The law uses the term ‘consent’ and not ‘informed consent.’ This means that the guidance on what constitutes consent is regulated by the specific discipline.

Ethical standards on informed consent

- Guideline 5.2 of the National Guidelines for Research involving Humans as Research Participants, 2014 adopted by the Uganda National Council for Science and Technology provides that,

‘Except as provided elsewhere in these guidelines, no researcher shall involve an individual person as a research participant unless the researcher has obtained ***informed consent*** of the individual or the individual’s authorized representative.’

- Despite it being a cornerstone of research ethics, as it serves to fulfil the research principles of respect, beneficence and justice, the limits of informed consent are not clearly defined - ***Xu, A., Baysari, M.T., Stocker, S.L. et al. Researchers’ views on, and experiences with, the requirement to obtain informed consent in research involving human participants: a qualitative study. BMC Med Ethics 21, 93 (2020)***

Ethical standards on informed consent

- Under Article 1 of the Nuremberg Code, 1947 – informed consent is explained as meaning that

‘the person involved should have legal capacity to give consent; should be so situated as to be able to exercise free power of choice, without the intervention of any element of force, fraud, deceit, duress, overreaching, or other ulterior form of constraint or coercion; and should have sufficient knowledge and comprehension of the elements of the subject matter involved as to enable him to make an understanding and enlightened decision.’

- The Belmont Report, 1979 provides that

‘Respect for persons requires that subjects, to the degree that they are capable, be given the opportunity to choose what shall or shall not happen to them. This opportunity is provided when adequate standards for informed consent are satisfied.’

It emphasises three aspects of informed consent: Information, Comprehension, and Voluntariness.

Information to provide during the informed consent process

- The laws of Uganda and the UNSCT Guidelines apply to both traditional field research and electronic research (Guideline 5.2).
- Guideline 5.3 provides for the information to be included in the informed consent form.
- Under Guideline 5.1 ‘informed consent is not just a form or a signature/mark/thumbprint but a process of information exchange between the researcher and research participants on the whole research process.’
- This implies that whatever is applicable to traditional field research should also apply to electronic research.

Electronic and digital signatures

- Section 6 of the The Electronic Transactions Act Cap 99 provides that ‘Where a law requires a signature or provides for consequences where a document is not signed, the requirement is fulfilled if an electronic signature is used.’
- An electronic signature is defined as ‘data in electronic form affixed to or logically associated with a data message, which may be used to identify the signatory in relation to the data message and indicates the signatory's approval of the information contained in the data message; and includes an advanced electronic signature as well as secure signature.’
- This means that once one signs electronically and the data can be linked to them, they are bound. One can therefore sign by simply clicking a box without reading as commonly seen in software agreements etc.

How to prove informed consent in electronic research

- The Electronic Signatures Act Cap 99 provides for electronic signatures and digital signatures – digital signatures are a type of electronic signatures where the identity of the person signing can be determined using private and public keys.
- However, whether it is a digital signature of other type of electronic signature, this clearly does not satisfy the requirement of informed consent as understood in research ethics, although it satisfies the evidential burden of the law.
- As such the focus is not on the signature and its validity but rather on whether the person understood the basics of the research and validly consented.
- In the case of *Mukoda alias Naigaga v International Aids Vaccine Initiative & 11 Ors* Human Rights Petition No. 305 of 2017 decided in 2020, the High Court emphasised the importance of informed consent and went beyond the signature to whether the researchers fulfilled their obligations under the Helsinki Declaration.

Third party alterations of electronic data

- Third party interventions in transmission of electronic data is a common concern.
- The concern is whether the very message sent is the very message that has actually reached the other person.
- Third party alterations can be in the form of man-in-the-middle-attacks.
- This highlights the importance of data security.

Identity of the person consenting in the era of AI and deepfake

- An important consideration in the validity of informed consent in electronic research is whether the person presumed to consenting is actually the one doing so.
- In these days of AI and deepfake, one can never be sure even if there is video evidence.
- Deepfake technology enables the manipulation of images, videos, audio, and even text to generate highly realistic synthetic content, including written material intended to mimic an individual's communication style, often without their consent. T. Kirchengast **Deepfakes and image manipulation: Criminalisation and control** *Information and Communications Technology Law*, 29 (3) (2020), pp. 308-323.
- So the issue is how to prove that the person you spoke to is the person you intended to speak to.
- AI is very crucial in research as its tools can be used to analyse large datasets, and automate tasks, but they should be used as tools to augment human expertise, not replace it. However, one must beware falsification of data issues and fake references.

HOW TO PROTECT CONFIDENTIALITY DURING ELECTRONIC RESEARCH

- The Computer Misuse Act Cap 96 criminalises a number of things if done through a computer, and the relevant ones to researchers are:
 - Section 11(1)(a) – criminalises unauthorised access to another person's data or information,
 - Section 11(1)(b) – criminalises unauthorised voice or video recording of another person;
 - Section 11(1)(c) – criminalises unauthorised sharing information about or that relates to another person without authorisation commits an offence
- Under section 11(7), the punishment is a fine not exceeding 15 million shillings or imprisonment for ten years or both
- Section 23 – unauthorised sharing of information about children – without parental consent etc commits an offence punishable by a fine of 15million or imprisonment of seven years or both

Confidentiality during electronic research

- These laws show the importance of obtaining informed consent during electronic research but also of ensuring confidentiality of research data.
- It is now criminal offence if data confidentiality is breached.
- Electronic process are however almost inherently vulnerable to internet attacks including unauthorised access to databases, man-in-the-middle-attacks, networking sniffing on unencrypted connections and third and by exploiting vulnerabilities in third-party vendors which all can occur during transfer of data.
- There is therefore need for more data security so that researchers avoid going afoul of the law and ethical principles.

ACCESS TO COMPUTERS/INTERNET AS AN INCLUSION/EXCLUSION CRITERIA

- Including internet access as an inclusion criterion in research is necessary for studies that rely on online data, platforms, or communication.
- However, this create a digital divide by excluding participants with limited access. This is a serious issue with countries with low internet penetration such as Uganda.
- Most importantly, it goes to the validity of the research findings – as well as generalisability.
- It may also go to community engagement – to what extent has the researcher involved less technologically advantaged community members.

DIGITAL COMPENSATION OF PARTICIPANTS

- Compensation of participants is an important issue in research ethics.
- With the adoption of mobile money technologies, mobile banking platforms, paying money is much easier than ever.
- Issues would arise when there is no easy access to such technologies by participants. How they will they get compensated?

COMMUNITY ENGAGEMENT IN ELECTRONIC RESEARCH

- Community engagement is a very important concept in research.
- Guideline 12.1 of the UNCST HSP Guidelines provide that '*Researchers shall make reasonable effort to involve community stakeholders in the research process, where appropriate, right from the inception of research to post research period.*'
- The UNCST's 'National Guidelines for Community Engagement in Research' 2022 indicate that community engagement is an opportunity for communities to participate in the design and conduct of research and enhances the relevance, ownership, and applicability of research findings.
- Since electronic research does not involve physical field visits and community engagements, the question of how community engagement will be done becomes important.
- Most communities in Uganda are rural based and do not have access to the internet – so how does one genuinely and meaningfully engage them electronically?

Community engagement in electronic research

- The Guidelines envisage using digital media like internet and mobile telephones (phone text) as well as Internet media e.g., social media, emails, websites, Facebook, X, WhatsApp as one of the ways of undertaking community engagement.
- However, the Guidelines envisage these to be used when reaching out to a broader community where a study is not under one geographical area or to a particular group of individuals. How about when the participants are a smaller group and in one area?
- Researchers employing electronic research methods should use technology to involve communities in the research process, from design to dissemination. This can range from researchers leading a study with community input to full community partnership where the community drives the research agenda.
- Using electronic research methods does not preclude physical engagements more especially at the design stage so that the research get to understand the community more and therefore determine the best technology to use – not the technology that is convenient to them, but that that is convenient to the communities.



CONCLUSION

- The rapid developments in technology have made research much easier. They have also similarly created major challenges in research.
- The challenges affect both the legal framework and the ethical framework. The law does not prohibit electronic research and indeed clearly regulates it through laws such as the DPPA, and the Computer Misuse Act.
- Issues affecting informed consent, privileging the views of those with access to computers, as well as the need to ensure confidentiality and data security online all becoming important.
- Researchers should be aware of the technological developments, the ethical challenges that arise from the use of technologies as well as the legal developments, and how all these issues enhance or diminish community engagement and work to ameliorate them.