Guidelines on the Treatment of Electronic Evidence in Criminal Proceedings

The Commonwealth

Guidelines on the Treatment of Electronic Evidence in Criminal Proceedings

The Commonwealth

Published by the Commonwealth Secretariat.

Contents

Background

In the Commonwealth Cyber Declaration 2018, the Commonwealth Heads of Government (CHOGM) committed, inter alia, to building the foundations of an effective national cybersecurity response and a cyberspace that supports economic and social development and rights online, and to promoting stability in cyberspace through international cooperation. They committed to establishing 'effective and proportionate domestic cybercrime and cybersecurity frameworks', to 'enable cross-border access to digital evidence' and to working 'towards common standards, harmonised legal approaches and improved interoperability'.

Ensuring that electronic evidence can be safely and securely relied upon in domestic criminal proceedings is central to achieving these aims. To this end, the Commonwealth Secretariat commissioned a Research Report on its *Model Law on Electronic Evidence* (2019) and convened an Expert Working Group (10–11 September 2019) which considered the findings of the Report. The outcomes and recommendations of the Expert Working Group were presented to law ministers at the Meeting of Commonwealth Law Ministers and Senior Officials (Sri Lanka, 4–7 November 2019), and law ministers agreed that the Commonwealth Secretariat could prepare 'guidelines on the use of electronic evidence in criminal proceedings' (Outcome Statement, para. 8). Draft guidelines were prepared and considered by a second Expert Working Group (24 March 2023), after which they were finalised and presented at the Virtual Meeting of Senior Officials of Commonwealth Law Ministries 23 November 2023 and the Meeting of Commonwealth Law Ministers and Senior Officials 2024 (Zanzibar, 4-8 March 2024). The guidelines were adopted as a Commonwealth guide at the latter meeting (Outcome Statement, para. 29).

The preparation of these guidelines[1] drew on a range of academic and practitioner sources, guides for legal practitioners and other international guidelines concerning electronic evidence, as well as the above-mentioned research report commissioned by the Commonwealth Secretariat as part of the implementation of the Cyber Declaration. The bibliography of this document contains some of the key sources that were relied upon.

1 Authored by Dr Micheál O'Floinn, Senior Lecturer in Criminal Law. University of Glasgow

1. Purpose and Scope

The purpose of this document is to assist and guide countries in creating processes for the reliable and secure treatment of electronic evidence in criminal proceedings. It does so while recognising and respecting the diversity of evidential frameworks across Commonwealth countries. It also acknowledges the challenges in effectively using electronic evidence and highlights the need to provide practical guidance for courts and other competent authorities handling such evidence in criminal proceedings. The guidelines thus seek to:

a. inform understandings of the concept of electronic evidence;

b. assist countries in the creation, implementation and adaptation of domestic rules of evidence and procedure applicable to electronic evidence;

c. underline the utility of electronic evidence in criminal cases, while also highlighting the risks associated with relying on this category of evidence and offering guidance on how to address these risks in criminal proceedings;

d. identify key principles and factors that should guide courts and other competent authorities in the use and management of electronic evidence.

These guidelines are non-binding and are thus to be applied only insofar as they do not conflict with national law.

2. Definitions

'Computer system' means any device or group of interconnected or related devices, one or more of which, pursuant to a program or other software, stores, transmits or otherwise processes electronic material.

'Electronic evidence' means any evidence derived from electronic material that may be used to prove or disprove a fact in legal proceedings.

'Electronic material' means any representation of data or of information that has been stored, transmitted or otherwise processed in a computer system.

'Metadata' refers to data about other electronic material which may reveal the origin and history of the material, and assist with identifying aspects, including relevant dates and times.

'Trust service' means an electronic service which facilitates:

a. the creation, verification and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services;

b. the creation, verification and validation of certificates for website authentication; or

c. the preservation of electronic signatures, seals or certificates related to those services.

3. Fundamental Principles

a. Electronic evidence should be admissible in electronic form in any criminal proceedings. Courts should not refuse to admit electronic evidence, or deny its legal effect, solely because it was generated, collected or presented in electronic form.

b. General rules of evidence should normally apply to electronic evidence as they do to other types of evidence. Nevertheless, heightened scrutiny may be required in applying certain admissibility rules, and rules for proof of evidence, due to the ease with which electronic evidence can be manipulated, distorted or erased.

c. Courts should seek to ensure a fair balance between the opportunities afforded to the prosecution and defence with respect to any reliance on electronic evidence in criminal proceedings.

d. It is for the finder of fact in any criminal proceedings to determine the ultimate probative value of electronic evidence, if any, in accordance with national law and rules of evidence.

4. Collection and Handling of Electronic Material

States should have clear procedures, protocols and guidance for those involved in the preservation, seizure, collection, handling and examination of electronic material and devices that may be utilised in criminal proceedings. These frameworks should ensure that the following general principles and good practices are followed by investigators, prosecutors and other competent authorities responsible for handling electronic material in criminal proceedings.

i. Any investigative actions undertaken in relation to any electronic material and devices are pursuant to law.

ii. Where devices are seized or otherwise procured, no action should be taken that changes data on a device that may be subsequently utilised in any way in criminal proceedings.

iii. The examination of devices should only be done by someone who is competent to do so, and who is able to explain their actions – and the implications of their actions – with respect to the device, to a court.

iv. An audit trail should be kept for all processes followed. Another qualified practitioner should be able to follow the audit trail and achieve the same results. So far as is practicable, any searching or processing of electronic material, as well as the data identified by that process, should be properly recorded. Records or logs should be made of all devices and electronic material seized or imaged and subsequently retained as relevant to the investigation.

v. Consideration should be given to the impact of any seizure of devices, and particularly the effect that any seizure may have on a business, organisation or individual. Any intrusion into the private lives of individuals should be justified and necessary, using the least intrusive means possible to obtain the material sought.

vi. Devices should not be seized as a matter of course, and the decision to do so should be a fact-specific decision to be made in every criminal investigation. Where feasible and practical in the specific circumstances of the case, investigators may be encouraged to image rather than seize devices, or obtain the relevant electronic material through other means, such as by way of production orders.

vii. Any law enforcement or prosecutorial duties to retain or preserve electronic material should specify the categories of material that are subject to retention or preservation, relevant periods and procedures to ensure that the material is retained or preserved in an appropriate and secure manner, and when destruction or return must be undertaken.

viii. Where devices are seized and it becomes apparent that they do not contain any relevant electronic material for the purposes of the investigation, they should be returned at the earliest opportunity.

5. Privileged Material

States should have a clear and explicit legislative framework for handling, accessing and analysing electronic material and devices that may contain legally privileged material, or material that is subject to other relevant privileges or immunities.

6. Disclosure

a. Any disclosure frameworks that apply in domestic criminal proceedings should be adapted, where necessary, to cater for electronic material in the disclosure process.

b. In particular, disclosure frameworks should.

   i. recognise that devices are capable of storing large volumes of electronic material, much of which may not be relevant for disclosure purposes;

   ii. specify the persons or authorities who are competent and responsible for conducting any sifts or other forms of review of electronic material, the procedures they must follow and permissible techniques and timeframes for fulfilling any disclosure obligations;

   iii. provide guidance for how to fulfil disclosure obligations where cases involve large quantities of electronic material, and where it may be impossible for investigators to examine every item of such material individually;

   iv. ensure that investigators, prosecutors or any other competent authorities with disclosure obligations must bear in mind the overriding obligation to ensure a fair trial of any suspect;

   v. incentivise timely consultations, where appropriate, between investigators and prosecutors or other competent authorities responsible for bringing criminal proceedings, to agree strategies for dealing with the electronic material that is relevant to the case and to determine what material must be shared with the defence;

   vi. seek to ensure a balance between the fair trial rights of the accused and the privacy and data protection rights of any complainants, witnesses and any relevant third parties. Where investigators or prosecutors decide that it is necessary to request or otherwise obtain electronic material from a complainant, witness or other third party, this should only be done when it is in accordance with domestic law, strictly necessary and proportionate.

7. Transmission of Electronic Evidence for Legal Proceedings

a. Electronic evidence should be submitted to courts in a secure and reliable manner, maintaining its integrity and following a clear chain of custody and transmission between collection and examination by investigators or experts and its use in court.

b. Electronic evidence should be collected, structured and managed in a manner that facilitates its transmission to other courts, where this may be necessary following the conclusion of the criminal proceedings.

c. Transmission of electronic evidence by electronic means should be encouraged and facilitated so long as it does not impact or risk jeopardising the cases for the prosecution or defence.

d. Systems and devices for transmitting electronic evidence should be able to ensure that the integrity of the evidence can always be maintained.

8. Best Evidence

a. Any domestic implementation of the 'best evidence' rule or the related 'original document' rule should be flexible and should not exclude electronic evidence solely because it is adduced as secondary evidence in the form of a physical or other form of copy.

b. Any domestic implementation of the 'best evidence' rule with respect to electronic evidence should not, however, be capable of being satisfied simply based on evidence that the computer system(s) used to generate the electronic evidence operated properly or reliably. Evidential presumptions concerning the operation or reliability of computer systems should not preclude assessments of, and challenges to, the integrity and reliability of electronic evidence in any domestic implementations of the best evidence rule.

9. Relevance

a. Courts should engage in the active management of cases involving electronic evidence to ensure that any evidence that is adduced or required is necessary and not excessive for the matters to be proved in the case.

b. Courts may require the assistance of recognised experts in the analysis of electronic evidence to assist in relevancy determinations.

c. Where courts utilise concepts of legal relevancy for addressing reliability concerns related to electronic evidence in admissibility determinations, they should ensure that the evidentiary requirements are defined with sufficient precision for parties to know what is required for the admissibility of the evidence.

10. Reliability and Authentication

a. States and/or their courts should provide guidance on any authentication requirements or other processes for satisfying burdens of production or proof applicable to electronic evidence in criminal proceedings.

b. The following factors may be considered relevant to authentication requirements.

   i. Whether the electronic material relied on in any criminal proceedings can be shown to be an accurate representation of the prevailing and existing state of that material at the time relevant to the legal proceedings.

   ii. Whether the electronic material has changed from the moment it was identified and collected as potential evidence for the criminal proceedings, and whether there is an accurate and reliable method of documenting any such changes, including the reasons for any such modifications.

   iii. Whether the continuity of the electronic material can be demonstrated between the moment in time when it was obtained for legal purposes and when it was submitted as an exhibit in the criminal proceedings.

   iv. Whether the techniques that were used to obtain, secure and process the electronic material can be tested and shown to have been appropriate for the purpose for which they were applied.

   v. Whether the provenance and integrity of the electronic material can be reliably demonstrated and are capable of being proved.

   vi. The value of trust services in establishing the reliability of electronic material.

   vii. The probative value of metadata.

c. If conviction in criminal proceedings depends on the authenticity of electronic evidence, the factfinder would need to be satisfied to the applicable standard of proof of its authenticity.

11. Evidential Presumptions

A number of states recognise rebuttable presumptions in relation to, for example, the operation of devices, the integrity of device outputs or the reliability of electronic evidence from certain official or third-party sources. While presumptions can serve to improve the efficiency of trial processes and help to focus parties on the main issues in a case, there is a risk that courts could be misled where presumed facts turn out to be false or are otherwise contestable.

a. States should review the conditions under which presumptions apply to electronic evidence, ensuring they are coherent, justifiable in light of modern computing technology, and do not unduly disadvantage any party in criminal proceedings.

b. States should ensure that trial procedures and disclosure processes provide parties to criminal proceedings with a practical opportunity to challenge the operation of any presumptions, where disproving the presumed fact is an essential feature of their case.

12. Admissibility of Electronic Evidence by Agreement

Where domestic rules of procedure allow for the admissibility of electronic evidence by agreement between the prosecution and defence, states should consider imposing validity requirements for such agreements, including that where the evidence is prosecution-led, the accused person(s): (i) were legally represented at the time of the agreement, (ii) provided informed consent and (iii) were aware of the nature and extent of the electronic evidence and the purpose for which it is to be adduced in the proceedings.

13. Admissibility of Electronic Evidence from Other Jurisdictions

a. Electronic evidence that is obtained from another jurisdiction should not be found to be inadmissible solely due to the foreign origin of the evidence, provided other relevant admissibility criteria in the receiving country can be satisfied.

b. States should seek to foster cooperation between its domestic authorities and foreign service providers, while ensuring that any electronic material that is received is (i) sent via secure, robust and reliable channels that can assure the continuity and integrity of the electronic material and (ii) through requests or orders that are lawful as a matter of domestic and international law.

14. Storage and Preservation

a. Where electronic evidence is to be stored pursuant to domestic law for the duration of the criminal proceedings, this should be done in a manner that preserves readability, accessibility, integrity, authenticity, reliability and, where applicable, confidentiality and privacy.

b. Electronic evidence should be stored with standardised metadata, where possible, so that the context of its creation is clear.

c. The readability and accessibility of any stored electronic evidence should be guaranteed over time, taking into account the evolution of information technology.

15. Archiving

a. Courts should archive electronic evidence in accordance with national law. Electronic archives should meet all safety requirements and guarantee the integrity, authenticity, confidentiality and quality of the data, as well as respect for privacy and data protection.

b. The archiving of electronic evidence should be carried out by qualified specialists.

c. Data should be migrated to new storage media when necessary to preserve the accessibility to electronic evidence.

16. Awareness-raising, Review and Training

a. States should promote awareness of the benefits and value of electronic evidence in criminal proceedings, as well as the risks of wrongful convictions or failed prosecutions where the evidence is mismanaged or not treated with due care and attention in the criminal process.

b. States should keep technical standards related to electronic evidence under review.

c. All professionals dealing with electronic evidence in criminal justice procedures should have access to the necessary interdisciplinary training for handling such evidence to the extent necessary for fulfilling their role and duties.

d. Through continuing professional development, judges, judicial officers, law enforcement and other legal practitioners should be kept abreast of the evolution of information technologies where this may affect the availability, reliability, utility, or value of electronic evidence.

Bibliography

Association of Chief Police Officers (2012), *Good Practice Guide for Digital Evidence*, ACPO, London

Bohm, N et al (2022), Briefing Note: The legal rule that computers are presumed to be operating correctly – unforeseen and unjust consequences *Digital Evidence and Electronic Signature Law Review*, Vol. 19, 123-127.

Chasse, K (2007), 'Electronic records as documentary evidence', *Canadian Journal of Law and Technology*, Vol. 6 No. 3, 141-162.

Christie, J (2023), 'The Law Commission and Section 69 of the Police and Criminal Evidence Act 1984', *Digital Evidence and Electronic Signature Law Review*, Vol. 20, 62-95

Council of Europe (2019), *Electronic Evidence in Civil and Administrative Proceedings: Guidelines and Explanatory Memorandum*, Council of Europe, Strasbourg

Council of Europe (2022), *Electronic Evidence Guide v 3.0*, Council of Europe, Strasbourg

Dennis, I (2020), *The Law of Evidence, 7th ed*, Sweet and Maxwell, London

Duranti, L, C Rogers and A Sheppard (2010), 'Electronic records and the Law of Evidence in Canada: The uniform electronic evidence Act twelve years later' (2010) *Archivaria*, Vol.70, 95-124

European Union Network and Information Security Agency (2015), *Electronic Evidence – A Basic Guide for First Responders,* ENISA, Athens

Grimm, PW, DJ Capra and GP Joseph (2017), Authenticating digital evidence *Baylor Law Review*, Vol. 69 No. 1, 1-55.

Mason S (2014), 'Electronic evidence: A proposal to reform the presumption of reliability and hearsay' *Computer Law & Security Review*, Vol 30 No. 1, 80-84.

Mason, S and D Seng (eds) (2021), *Electronic Evidence and Electronic Signatures* 5th ed Institute of Advanced Legal Studies for the SAS Humanities Digital Library, London, UK

Munday, R (2018) *Cross & Tapper on Evidence 13th ed*, OUP, Oxford

Ó Floinn, M (2019), *Revision of the Model Law on Electronic Evidence: Background Paper* Commonwealth Secretariat, London

Ó'Floinn, M and D Ormerod (2012), 'Social networking material as criminal evidence' *Criminal Law Review,* Vol 7 No. 7, 486-512.

Pattenden, R (2008), 'Authenticating 'things' in English law: Principles for adducing tangible evidence in common law jury trials' *International Journal of Evidence & Proof*, Vol. 12 No. 4, 273-302.

Pattenden, R (2010), 'Machinespeak: Section 129 of the Criminal Justice Act 2003' *Criminal Law Review*, Vol. 5, 623-636.

Quinn, K (2001), 'Computer evidence in criminal proceedings: farewell to the ill-fated s. 69 of the Police and Criminal Evidence Act 1984', *International Journal of Evidence & Proof*, Vol. 5 No. 3, 174-187.

Smith, JC (1981), 'The admissibility of statements by computer' *Criminal Law Review,* 387.

UK Attorney General's Office (2024), *Attorney General's Guidelines on Disclosure*, Attorney General's Office, London

United Nations Office on Drugs and Crime (2021), *Practical Guide for Requesting Electronic Evidence Across Borders*, UNODC, Brussels

Walden, I (2016) *Computer Crimes and Digital Investigations 2nd ed*, OUP, Oxford

Commonwealth Secretariat
Marlborough House, Pall Mall
London SW1Y 5HX
United Kingdom

thecommonwealth.org

The Commonwealth

D20163