The way forward

Biasiotti, Maria Angela ; Cannataci, Joseph A.; Mifsud Bonnici, Jeanne Pia; Tudorica, Melania

Published in:
Handling and Exchanging Electronic Evidence Across Europe

DOI:
10.1007/978-3-319-74872-6_18

Chapter 18
The Way Forward: A Roadmap for the European Union

Maria Angela Biasiotti, Joseph A. Cannataci, Jeanne Pia Mifsud Bonnici, and Melania Tudorica

Abstract The contributions describe the final Road Map for the realization of the harmonized framework on Electronic Evidence Treatment and Exchange. It is against a complex background that this "Roadmap" needs to be understood as it takes all challenges, including legal, operational, technical and data protection, forward and proposes ways to take action on a national and on a European level while taking into account various important aspects such as the actors involved. It is important to reiterate that no one action alone will solve the ensemble of challenges as regards the collection, preservation, use and exchange of electronic evidence. The actions need to be taken together for changes to be more effective. The Roadmap is aimed at showing the way forward for creating a Common European Framework for the systematic, aligned and uniform application of new technologies in the collection, preservation, use and exchange of evidence in criminal proceedings.

18.1 Introduction

It is against a complex background that this "Roadmap" needs to be understood as it takes all challenges, including legal, operational, technical and data protection, forward and proposes ways to act on a national and on a European level while considering various important aspects such as the actors involved. It is important to reiterate that no one action alone will solve the ensemble of challenges concerning the collection, preservation, use and exchange of electronic evidence. The actions must be taken together for changes to be more effective. The Roadmap is aimed

M. A. Biasiotti (✉)
CNR, Institute of Legal Information Theory and Techniques, Florence, Italy
e-mail: mariangela.biasiotti@ittig.cnr.it

J. A. Cannataci · J. P. Mifsud Bonnici · M. Tudorica
University of Groningen, Security, Technology and e-Privacy (STeP), Groningen, The Netherlands
e-mail: j.a.cannataci@step-rug.nl; g.p.mifsud.bonnici@step-rug.nl; m.tudorica@step-rug.nl

M. A. Biasiotti et al. (eds.), *Handling and Exchanging Electronic Evidence Across Europe*, Law, Governance and Technology Series 39,
https://doi.org/10.1007/978-3-319-74872-6_18

at showing the way forward for creating a Common European Framework for the systematic, aligned and uniform application of new technologies in the collection, preservation, use and exchange of evidence in criminal proceedings. The original Roadmap, as it was submitted to the European Commission,[1] was a policy brief aimed at policymakers that incorporates standardised solutions for a Common European Framework concerning the collection, preservation, use and exchange of electronic evidence to enable policymakers to define an efficient regulation for the treatment and exchange of electronic evidence. In this way Law Enforcement Agencies (LEAs), as well as the judiciary, prosecutors and lawyers practising in the criminal field may rely on a Common Framework that allows them to collect, preserve, use and exchange electronic evidence according to common standards and rules while fostering a sociological approach that is complementary to the legal, enforcement and technical approaches. The Roadmap furthermore provided a ground for further research considering that there still are areas that require further research considering that they are relatively 'young', such as virtual currencies. This chapter provides an extract of that Roadmap with an overview of the status quo of the most important challenges when dealing with electronic evidence, as well as suggestions for a way forward.

While there have been certain initiatives to bridge the gaps in the current framework of dealing with electronic evidence, including by the EU and Council of Europe, limitations remain that causes a variety of law enforcement challenges. Current national and international legal frameworks are insufficient to meet with the needs and solving the shortcomings is not merely a matter of introducing new agreements but is more complex, needing new theoretical frameworks and the collaboration of a large variety of actors. Considering the very nature of electronic evidence and rapidly evolving technologies and crimes it is important to act now and to address the challenges within the current system by realising a Common European Framework for the collection, preservation, use and exchange of electronic evidence. This framework should strike a balance between effective law enforcement on the one hand and proper protection of citizens' fundamental rights on the other hand considering that certain investigative measures that involve modern technologies can have a high impact on the suspect's fundamental rights Aulitano (2016). Especially the investigative measure that takes place in a digital environment can have a high impact on fundamental rights, as they allow for the gathering of a high volume of (personal) information through different channels.

Currently evidence is exchanged in a cross-border dimension directly from a competent authority of a Member State to a competent authority of another Member State or via international actors such as Interpol and Europol. However, there is a lack of specific rules regulating the collection, preservation, use and exchange of electronic evidence. The latter is of utmost importance considering the very nature of electronic evidence in that it may be stored or located anywhere in the world. Traditional means for international cooperation in crime prevention and

[1] EVIDENCE project, Deliverable 9.2—Roadmap.

prosecution are no longer sufficient, considering this nature of electronic evidence. There is furthermore an emerging need for a common language or terminology to be used in all relevant activities within Europe. Rules and cooperation for the management of electronic evidence are necessary to re-conceptualise evidence location including issues concerning direct access to extraterritorial data by law enforcement authorities as an increasing number of crimes involve geo-distributed electronic evidence, not only for cybercrime but for all crimes in general. Traditional means for international cooperation in crime prevention and prosecution are not sufficient for a timely response for obtaining volatile electronic evidence. When it comes to the exchange of electronic evidence, further cooperation is necessary. Considering the volatile nature of electronic evidence, broad security perspective and collaborative investigation activities between the different actors are necessary within the Common European Framework. Internationally agreed mechanisms for preservation, supply and exchange of electronic evidence in criminal matters must be strengthened and evidence management by means of ICT needs to comply with national laws for the evidence to remain authentic and trustworthy and to be admissible in national courts.

18.2 Status Quo

The collection, preservation, use and exchange of electronic evidence can be analysed from different perspectives, including legal, operational, technical, and data protection, while bearing in mind sociological and other relevant aspects. All perspectives taken together are necessary to improve the current way of handling electronic evidence in Europe and beyond. The EVIDENCE project analysed the status quo concerning the collection, preservation, use and exchange of electronic evidence and identified many complexities in the current system of handling electronic evidence. This includes legal gaps, realities and difficulties law enforcement is faced with, evolving crimes, evolving technologies and technical challenges, the enormous number of actors involved and trustworthiness, ethical issues, data protection issues, practical challenges such as authorisation, chain of custody and documentation, etc. The challenges in the current way of handling electronic evidence are addressed in the Roadmap.[2] An extract of the status quo analysis is provided in this paragraph.

18.2.1 Law and Policy

The introduction and extensive use of ICT has generated new forms of crimes or new ways of perpetrating them, as well as new types of evidence. Although all kinds

[2]EVIDENCE project, Deliverable 9.2—Roadmap.

of evidence must be handled according to criminal (procedural) laws, the 'new' types of evidence need additional and specific ways of handling to maintain the authenticity and integrity of the electronic evidence. The very nature of data and information held in electronic form makes it easier to manipulate than traditional forms of data. When acquired and exchanged the integrity of information must be maintained and proved, i.e. demonstrated that the electronic evidence has not been altered since the time it was created, stored or transmitted. Legislations on criminal procedures in many European countries were enacted before these technologies appeared, thus not considering them. Therefore, the handling of electronic evidence, as well as the exchange between EU Member States jurisdictions, are based on different criteria and uncertain, not harmonised procedures. What is missing is a Common European Framework to guide policy makers, LEAs and legal authorities when dealing with electronic evidence handling and exchange. There is a need for a common background for all actors (policy makers, LEAs, judges, lawyers) involved in the electronic evidence lifecycle, including a common legal framework and standardised procedures regulating the collection, preservation, use and exchange of electronic evidence.[3]

European legislation adds important value to the national legal systems, creating a common framework to prevent and ban crimes, considering that the most serious types of organised crime are committed across borders. It furthermore makes the fight against crime more efficient by adopting minimum standards in the criminal field, as well as in the cybercrime area. It thus strengthens the importance of a common effort in preventing and combating crime, especially cybercrime, by creating a common framework to foster and improve cooperation between states. Many guidelines and technical standards have been produced by LEAs, (European) institutions and (national) policy makers. These guidelines and standards are aimed at providing support and guidance in handling and examining electronic evidence. Many guidelines and best practices answer the need for LEA personnel to acquire necessary competencies and knowledge to fill the gap of standardised procedures across agencies, as well as the lack of specific legislation governing the collection, analysis, preservation, use and exchange of electronic evidence.[4] These legal instruments and guidelines are however a patchwork of documents and no comprehensive international or European legal framework relating to (electronic) evidence exists. Parties involved rely on national law when it comes to the collection, preservation, use and exchange of (electronic) evidence, which makes dealing with electronic evidence internationally difficult. Moreover, national criminal laws have been written ages ago, long before there was such a thing as the internet and modern technologies, which could provide electronic evidence. While it is true that some countries have adapted their legislation to address technological developments, others rely on traditional laws and apply them to electronic evidence as well. There are thus big differences in national legislation and approach. Evidence

[3]EVIDENCE D2.1 EVIDENCE semantic structure, pp. 11, 15.

[4]EVIDENCE D2.1 EVIDENCE semantic structure, p. 20.

rules vary considerably even amongst countries with similar legal traditions. In certain countries traditional investigative powers might be general enough to apply to electronic evidence while in other countries traditional procedural laws might not cover specific issues regarding electronic evidence, making it necessary to have additional legislation. In certain countries there are defined rules as to admissibility of evidence in Court while in other countries admissibility is flexible. In all cases legislation requires a clear scope of application of powers and sufficient legal authority for actions.

While there is no comprehensive international or European legal framework relating to electronic evidence, several international and European legal instruments and policy documents are relevant to electronic evidence. This includes the European Union (EU) legal framework and guidelines, but more importantly the legal instruments and documents by the Council of Europe. In cybercrime, the Council of Europe's instruments are the legal framework of reference for combating cybercrime. The Council of Europe Convention on Cybercrime[5] (Cybercrime Convention) remains the main (and only) international treaty that defines the substantive elements that lead to some cyber activities to be classified as crimes; and which has procedural provisions that allow for the prevention, detection and prosecution of these activities. Although electronic evidence may not necessarily result from cybercrime, this is the main framework for reference in this area that offers many provisions to enhance investigations where electronic evidence is involved. The development of new communication and information systems in criminal justice and their use in most of individuals' daily activities has transformed the processes of information and evidence exchange. The increasing production of electronic data because of this widespread use of ICTs, but also the use of new technologies in the commission of old and new crimes (cybercrimes), contribute to make the collection and exchange of electronic evidence increasingly relevant in national criminal justice. This evolution and the gradual digitisation of the means necessary to collect and analyse electronic evidence has not been accompanied by a consistent and uniform evolution of the legal frameworks across Europe. Different rules and practices regarding the collection, preservation, use and exchange of electronic evidence exist in the European countries.[6] Given the increasing use of digital devices in daily activities the attention for electronic evidence in the European and national legislation is expected to increase. To prevent more fragmentation and even more different rules and practices it is necessary to address the issue as soon as possible and to go for a more harmonised approach to facilitate international cooperation in cross-border crimes.

Major challenges and shortcomings of the legal frameworks within the EU Member States, which include legal and data protection issues, problems with law enforcement, particularly concerning cross-border cases when evidence needs to be collected abroad or exchanged with competent authorities from another jurisdiction, and technical issues concerning training and technical capabilities. Effective leg-

[5]Convention on Cybercrime [2001] ETS 185.

[6]See EVIDENCE Deliverable 3.1—Overview of existing legal framework in the EU Member States.

islation and law enforcement should include an effective legal framework, access to investigative tools and techniques, training and technical capabilities and best practices policies that ensure proportionality between the protection of privacy and infringements for legitimate crime prevention and control.[7]

18.2.2 Data Protection

In a digitalised world, the use of electronic evidence becomes increasingly important in criminal proceedings. To effectively prosecute a crime, LEAs must adapt to this situation by working with the electronic evidence generated by the ubiquity of these new technologies and by using digital technologies themselves to collect evidence. Those investigative measures can have a high impact on the suspect's fundamental rights, especially in a digital environment, which allows collecting (personal) information through different channels. Consequently, there must be a balance between effective law enforcement on the one hand and proper protection of citizens' fundamental rights on the other hand. A European legal framework comprehensively addressing data protection issues related to the collection of electronic evidence does not exist. There is a need to include specific safeguards in current legislative frameworks to address the shortcomings. A Common European Framework should set up a minimum standard of privacy safeguards to be established in relation to the use of certain means of collecting electronic evidence. It should furthermore include a definition of electronic evidence, which could act as a basis to regulate certain investigative measures that were identified to have an effect on privacy related fundamental rights and establish technical standards and non-binding guidelines for the use of electronic technologies, which could be developed by a future high-level expert group being set up by the EU. From a data protection perspective, a Common European Framework should also seek to set-up rules on minimum data protection standards that must be met during the life-cycle of electronic evidence. This applies to both privacy safeguards and data security safeguards, particularly safeguards against alteration of electronic evidence. Non-binding guidelines regarding privacy safeguards and data security rules on a practical level are necessary to assist achieve an adequate level of data protection.

18.2.3 Actors

Fragmentation does not only exist in the legal framework, but is also reflected by the vast number of actors involved. On an international level there are several actors

[7]For more information on the legal status quo see: EVIDENCE Deliverable 3.1—Overview of existing legal framework in the EU Member States and EVIDENCE Deliverable 3.2—Status quo assessment and analysis of primary challenges and shortcomings.

involved, such as Interpol, Eurojust, Europol and its EC3 cybercrime centre and Joint Cybercrime Action Taskforce (J-CAT), CEPOL and ENISA. However, when we look at national level the number of actors involved in one way or another becomes numerous. Certain public and private actors and actors providing technical solutions and assistance have a direct interest in electronic evidence. These are process actors who make up the supply and demand for technologies and services and context actors who play an indirect role in electronic evidence in a broader political, social or economic context. Process actors include LEAs, SIS, the judiciary, digital forensic experts, etc. Context actors include international organisations and legislative bodies, research organisations, human rights organisations, the media, etc. One of the challenges, considering this vast number of actors involved, is that actors are not always in agreement considering the different interests involved and that the actors do not always coordinate with each other. Research further shows that there is a general mistrust within the judiciary that generally comes from a lack of necessary knowledge and competencies and a lack of professionalisation concerning digital forensics. Because of the (potential) global nature of electronic evidence, cultural differences in dealing with electronic evidence may also provide a challenge for law enforcement. These challenges can be addressed by mandatory training and education, certification, building bridges between the private and public sector, raising awareness, validation of tools, investing in digital forensic tools, etc.[8]

18.2.4 Law Enforcement

The challenges law enforcement is faced with, which are plentiful, are mostly legal challenges considering that LEAs are left to operate in a field of patchwork solutions, particularly concerning cross-border access to data, data retention, etc. While industry continues to push boundaries, LEAs are left playing catch up and manoeuvering their way through a highly uncertain and politically sensitive landscape filled with legal lacunae. Among other things, in an increasingly globalised online environment, the collection and exchange of electronic evidence is hampered by outdated and lengthy mutual legal assistance practices no longer adapted to today's realities. Legal lacunae hamper international law enforcement cooperation. For example, the invalidation of the EU Data Retention Directive, as well as a lack of international consensus regarding cross-border access to data, has led to quite some uncertainty for law enforcement investigating crimes in the online environment. The need for modernisation efforts in the field of international police and judicial cooperation are therefore necessary. The legal lacunae mostly need to be addressed

[8]For more information on the 'market' (actors, obstacles, facilitating factors) see: EVIDENCE Deliverable 7.1—Report on prima facie size of the market; EVIDENCE Deliverable 7.2—Map on obstacles and facilitating factors before validation and EVIDENCE Deliverable 7.3—Workshop Mapping obstacles and facilitating factors after validation.

by legal solutions. However, apart from legal solutions, professionalisation in the field of digital forensics is necessary. Digital forensic practitioners have expressed an interest for their field of expertise to reach a similar level of professionalism and recognition as, for instance, the field of DNA analysis. This would, however, require a reassessment of the potential regulation of digital forensics professions to ensure that practitioners meet a certain standard. Furthermore, as these practitioners often rely on automated digital forensic tools for the acquisition and analysis of electronic evidence, these tools should ideally be subject to validation procedures to ensure that they are fit-for-purpose. Lastly, there are currently no universal standards particularly applicable to digital forensic labs. Thus, it is also worth considering the development of an accreditation procedure to ensure digital forensic labs meet certain pre-determined quality levels across Europe.

As law enforcement is not the sole actor within the electronic evidence domain, the importance of 'building bridges' between LEAs and other stakeholders, including the public, policymakers, the private sector and the judiciary cannot be understated. Therefore, collaboration between LEAs and these other stakeholders also needs to be addressed. Particularly towards the public, that entrusts LEAs with the powers and resources to fulfil their mandate, LEAs should continue to expand their efforts in increasing transparency and accountability regarding their activities and spending. By providing statistics and documented case examples of law enforcement activities and needs, LEAs can provide the evidence-basis for an informed public debate upon which policymakers can, in turn, base their decisions. Furthermore, LEAs are increasingly confronted with evidence that has been collected and analysed by others stakeholders, particularly private companies, other public sector entities and citizens. LEAs will need to continue developing best practices in recognition of the fact that trustful collaboration with other actors is of essence in this field. Finally, as the examined cases and the evidence collected by LEAs is aimed to be brought before court to prosecute wrongdoers, the technical competences of prosecutors and judges to understand the electronic evidence process are also key. LEAs should aim to further strengthen their communication channels with those in the justice system, as this can contribute to enhancing the understanding of digital evidence within the judiciary, thereby potentially also alleviating LEAs from unnecessarily burdensome analysis requests.[9]

[9]For more information on the law enforcement status quo see: EVIDENCE Deliverable 6.1—Overview of the existing mechanisms and procedures for collection, preservation and exchange of electronic evidence by law enforcement agencies within the European Union and beyond; EVIDENCE Deliverable 6.2—Status quo assessment and analysis of primary challenges and shortcomings and EVIDENCE Deliverable 6.3—Identification of best practices and guidelines to be integrated into a comprehensive European Framework.

18.2.5 Technical Standards

The EVIDENCE project provided an overview of existing standards for the treatment and exchange of electronic evidence, also considering tools that are thoroughly tested and generally accepted in the digital forensics field in the EU Member States context. In this regard the lifecycle of electronic evidence and the main processes of the investigation phase in which a potential electronic evidence is identified, collected, and acquired and then safely preserved were mapped. Based on this map, a Digital Forensic Tools Catalogue was developed, which can become a point of reference within the forensic community, that will allow forensics experts to determine the most suitable tool for their case and to identify a similar or comparable tool for conducting a dual-tool validation.

The EVIDENCE project furthermore provided an overview of existing procedures for exchanging electronic evidence at national and European levels and proposed a standard for representing data and metadata involved in the exchange process and formal languages for their representation and it introduced a cloud platform for implementing the exchange process, listing the main features that this platform should have and putting the focus for a desirable integration with other existing platforms already in place and managed by international or European public bodies.

The EVIDENCE project finally produced and implemented a Proof of Concept (PoC) application on the electronic evidence exchange, persistence and support for maintaining a detailed chain of custody. The proposed architecture follows the reasoning of the goal-oriented analysis and considers the results of the analysis of existing systems of important stakeholders (such as Eurojust, Europol and INTERPOL). The implementation of the PoC (application and library) is designed to fill the gap of capturing the investigation actions performed during the lifecycle of a judicial case. The PoC facilitates this process by providing a structure that guides the forensic investigators and a representation language that enables serialisation of the investigation metadata, which also means packaging, sharing, reproducibility of results and in general facilitating exchange of electronic evidence. Additionally, using a structure representation language that has been approved by the forensics community would facilitate the integration of this technology with electronic evidence exchange mechanisms and systems in place. The aim of the PoC is not to replace or attempt to compete with existing systems, but rather to fill the gaps of functional and data format heterogeneity of existing systems by using standard, semantically rich protocols such as the DFAX language.

One of the main challenges is that the electronic evidence exchange standards needs the involvement of the different stakeholders to be a success. From a strictly technical point of view, it is important to convince actors in forensic tools development to extend or adapt their software to this news standard.[10]

[10]For more information on the technical status quo see: EVIDENCE Deliverable 4.1—Overview of existing standard for treatment and exchange of electronic evidence; EVIDENCE Deliverable

18.3 Strategic Goals

Based on the challenges and shortcomings concerning the collection, preservation, use and exchange of electronic evidence as mentioned in the previous paragraph and in the previous chapters strategic goals can be drafted for realising a Common European Framework for the application of new technologies in the collection, preservation, use and exchange of electronic evidence. These strategic goals include further research, enhancing legislation, enhancing law enforcement and professionalising digital forensics, enhancing technical standards and enhancing trust among actors and stakeholders. These goals or objectives are reflected below and can be taken forward to identify actions to be taken for realising the Common European Framework within a Roadmap. Actions include regulatory action, non-legislative measures and challenges that require further reflection, which must be addressed by a variety of actors.

18.3.1 Enhancing Legislation

One of the major objectives of the Roadmap is to enhance the legal framework. An enhanced legal framework will not only provide a legal basis and thus more clarity, but it will also improve law enforcement considering that many of the law enforcement challenges must be addressed primarily through legal action. Research showed that there is no comprehensive legal framework, no legislative harmonisation, but instead, a patchwork of legislation implemented differently among Member States. Existing legislation does furthermore not address the specific aspects of electronic evidence, which is aggravated by rapidly developing technologies, leaving legislation lagging behind. Certain issues, such as investigations in the cloud, are not regulated at all or not sufficiently regulated. This may cause legal and practical uncertainty, but also problems with (international) cooperation and law enforcement. The application of general rules of evidence may not always be sufficient in the collection, preservation, use and exchange of electronic evidence because of the specific nature of electronic evidence. A legislative framework should include clear and precise legal basis, uniform definitions, concepts and standards, best practices policies that ensure proportionality between protection of privacy and infringements for legitimate crime prevention and control, and will facilitate a more efficient cooperation. Legislation requires a clear scope of application of powers and sufficient legal authority for actions. Legal action requires, primarily, political will and commitment, which is why most of the legal actions also require political

4.2—Status quo assessment and analysis of primary challenges and shortcomings; EVIDENCE Deliverable 5.1—Technical specification document and guidelines; EVIDENCE Deliverable 5.2—First evidence exchange application prototype; EVIDENCE Deliverable 5.3—Workshop results and final technical specification document and guidelines.

action. The Roadmap consists of recommendations to build, improve and strengthen existing legislation in the field of electronic evidence to enhance legislation.

18.3.2 Enhancing Law Enforcement and Professionalising Digital Forensics

The second major objective of Roadmap is to enhance law enforcement, including professionalisation in the field of digital forensics. While most of the law enforcement challenges, which are plentiful, would primarily find a solution through legislative action, there are several actions that must be taken within the LEA community and the digital forensics community. Law enforcement needs to, among other things, provide feedback and input, both quantitative and qualitative, for legislation and guidelines to mitigate the negative impact of legislation to make investigations more efficient and effective. Enhancing law enforcement also includes professionalising the sub-discipline of digital forensics to achieve a certain level of professionalism and recognition within this young field. Regarding digital forensics, there is a call for achieving a certain level of professionalism and recognition. While certain practitioners might fear that standardisation efforts may hamper innovation, there is a consensus that this is only the commencement phase of a lengthy standardisation process. Professionalising digital forensics requires a reassessment of the potential regulation of digital forensics professions to ensure that practitioners meet a certain standard. These practitioners often rely on automated digital forensic tools for acquisition and analysis of digital evidence. Therefore, these tools should be subject to validation procedures to ensure they are fit-for-purpose. Furthermore, there are no universal standards particularly applicable to digital forensic labs. The development of an accreditation procedure to ensure digital forensic labs meet certain pre-determined quality levels would aid in achieving a universal standard. The Roadmap consists of recommendations to build, improve and strengthen existing procedures and law enforcement to enhance law enforcement and professionalise digital forensics. Professionalisation of digital forensics includes regulation and certification of the profession and training, validation of digital forensic tools, accreditation of digital forensics labs and building bridges between different actors. Improving and strengthening law enforcement includes collaboration with the public, policymakers (increasing transparency and accountability), the private sector, the judiciary and eventually modernisation of international cooperation (coordinated operations and JITs, digitisation of MLA and modernisation of international law).

18.3.3 Enhancing Technical Standards

A Common European Framework for the application of new technologies in the collection, preservation, use and exchange of electronic evidence cannot be effective without enhancing technical standards. The Roadmap includes recommendations

for a standard electronic exchange platform and language to represent a wide range of forensic information and processing results that is becoming an essential need in the forensics community. This includes a standard for representing data and metadata involved in the exchange process and formal languages for their representation. It also introduces a cloud platform for implementing the exchange process, which includes features such as cryptographic control and malware protection. The use of the standard DFAX, that leverages CybOX and the Unified Cyber Ontology, is recommended for representing metadata and describing in a detailed way all technical and legal forensic information. Presently, the DFAX and the related formalisms are not developed sufficiently, however, they have been designed for focusing on the extensibility and are therefore adaptable for covering all possible information needs for representing forensics investigations.

18.3.4 Enhancing Trust

Enhancing legislation and law enforcement cannot take place without support from all the actors involved. Challenges such as mistrust, security and cultural differences would stand in the way of implementation. The Roadmap therefore also includes supporting action from an ethical and social perspective to create awareness among actors, provide training of actors, etc. to enhance trust in and within the judiciary. The Roadmap consists of recommendations to build, improve and strengthen trust in and among judicial actors.

18.3.5 Further Research

Certain areas require further research before any action can be taken. More knowledge, for example, about (but not limited to) crypto-currencies, the Internet of Things and cloud computing is necessary before proper legislative and other measures can be taken in this regard. The final major objective of the Roadmap therefore is conducting further research and considering the results within a Common European Framework. Few areas have been identified by the EVIDENCE project as requiring further research. This includes constitutional limitations. Different constitutional traditions of the Member States lead to divergent implementation of international legislation and application of privacy and data protection principles. For better implementation of EU legislation, further insight in the constitutional traditions in the 28 Member States is required. Further research also needs to be conducted about data retention legislation in the Member States after the annulment of Directive 2006/24/EC by the Court of Justice of the EU (CJEU). Rules and procedures are mostly applied by LEAs. Input from this very important actor on how laws negatively impact investigation and prosecution, how severe this impact is and how frequently it occurs is therefore very important to improve investigative

techniques procedures and rules. Once there is a better understanding of these issues, legislation and policies may be developed more fit-for-purpose. The Roadmap consists of recommendations for further research.

18.4 Roadmap

The original Roadmap can be seen as a policy brief to guide law- and policymakers, law enforcement and other stakeholders when dealing with electronic evidence. This paragraph provides an extract of this Roadmap for realising a Common European Framework for the collection, preservation, use and exchange of electronic evidence, which is of the utmost importance considering the growing variety of electronic evidence used in criminal trials across the globe. If we want to realise this Common European Framework certain strategic goals or objectives must be met, including, amongst other things, enhancing law enforcement and enhancing the legal framework as discussed in the previous paragraph. These objectives can be met by providing solutions or actions for addressing certain challenges on a short, medium or long term. The objectives are interconnected and can be reached by fulfilling a minimum set of requirements, which will provide output (legislation, guidelines, etc.) generated by certain actors. By interconnected, we mean that no one action alone will solve the ensemble of challenges concerning the collection, preservation, use and exchange of electronic evidence. The actions must be taken together for changes to be more effective. Furthermore, all actions, whether they are short, medium or long term, need to start simultaneously and feed into each other while certain actions are expected to finish sooner rather than others, meaning on a short, medium or a term. By addressing the challenges by taking the actions suggested in the Roadmap, the objectives will be met and the Common European Framework for the collection, preservation, use and exchange of electronic evidence will be realised. Figure 18.1 shows that the solutions provided on a short, medium and long term will feed into each other and together will form the Common European framework for electronic evidence.

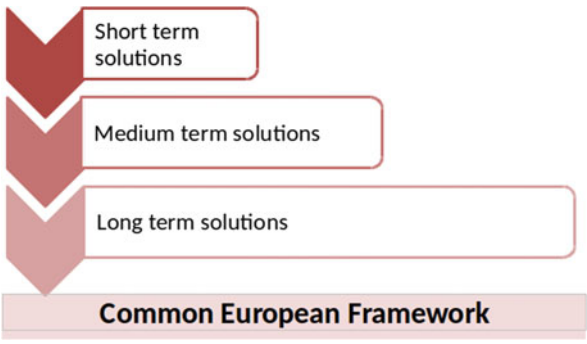

Fig. 18.1 Short, medium and long term solutions for the Common European Framework

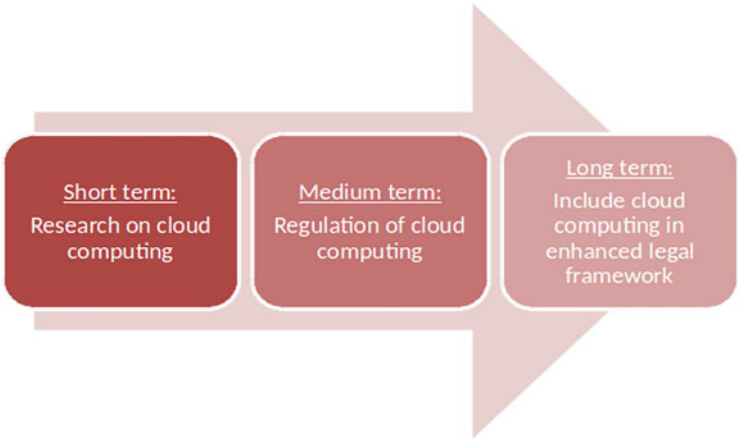

Fig. 18.2 Short, medium and long term solutions for addressing cloud computing issues

One might wonder why certain objectives and challenges are repeated on multiple levels, i.e. on a short, medium and long term. For example, 'enhancing law enforcement' is a short term, as well as a long-term objective. While the overall objective is indeed enhancing law enforcement, this may be achieved by a variety of solutions, some of which will take longer to achieve than others. Concerning challenges to reach the objectives, certain challenges need action on multiple levels. Figure 18.2 shows how one challenge, namely 'cloud computing', needs to be addressed on a short, medium and on a long term. On a short term, the subject needs to be further researched. The results of this research must be considered when regulating the subject before it can be included in the enhanced legal framework on the long term. The same goes for the MLA procedure, which will also be addressed on a short, medium and long term. On a short term, the challenge will be addressed by enhancing international cooperation and JITs, while on a medium term the MLA procedure will be digitised and on a long term the MLA procedure challenge will be addressed by modernising international law.

The Roadmap provides ten objectives for realising the Common European Framework for electronic evidence. Figure 18.3 shows the ten objectives and corresponding challenges, which are addressed in the Roadmap. Figure shows, again, the interconnected nature of the objectives and that only all actions taken together will realise the Common European Framework.

On a short term, the first steps in enhancing law enforcement will be taken by addressing three challenges; the MLA procedure, the realities of modern investigations and forensic readiness of the private sector. Moreover, on a short term, further research on many challenges will be conducted for the results to be considered on a medium and long term. The short-term solutions will thus feed into the medium and long-term solutions. On a medium term four objectives will be met by addressing the corresponding challenges, which will feed into the long-term

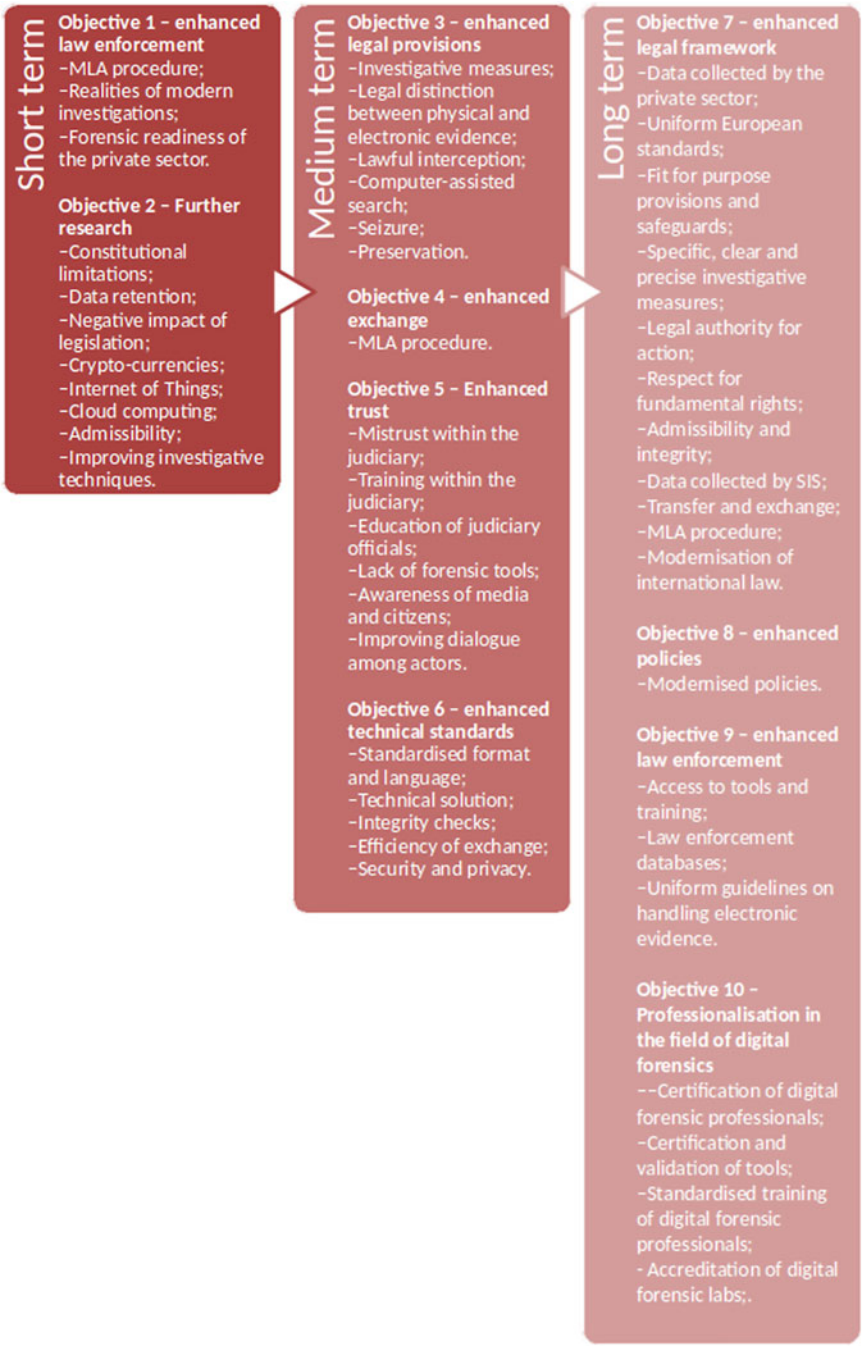

Fig. 18.3 The ten objectives and corresponding challenges which are addressed in the Roadmap

solutions where the final four objectives will be reached. As explained above, while certain objectives or challenges may be the same, the output or actions are different depending on what may be achieved within a certain timeframe.

Considering the status quo and the challenges found therein, as well as the strategic goals or objectives to improve the current way of handling electronic evidence, several solutions or actions may be provided for realising a Common European Framework for the application of new technologies in the collection, preservation, use and exchange of electronic evidence. The aim of the Common European Framework is to improve the efficiency of investigations and judicial procedures while maintaining adequate safeguards aimed at protecting relevant fundamental human rights and respecting clear standards of conduct. The objectives include conducting further research and enhancing law enforcement, legislation, policies, trust, technical standards and digital forensics and are divided in many actions that must be addressed on a short, medium or long term to reach the objectives. All actions need to start as soon as possible and preferably all at the same time. The short-term solutions are expected to be addressed in 2–3 years; the medium-term solutions in 3–4 years and the long-term solutions in 5–6 years. It needs to be noted that no one action alone will solve the ensemble of challenges identified. The actions must be taken together for changes to be more effective. All actions together will lead us to the Common European Framework for electronic evidence.

18.4.1 Short-Term Solutions

The short-term solutions are based on two major objectives, namely enhanced law enforcement and further research. Enhancing law enforcement is the major objective of the Roadmap considering that LEAs are the most important actors involved with electronic evidence. Law enforcement needs to work with the rules and procedures provided to them by law- and policymakers. Input from this very important actor is therefore of the essence. While most actions improving rules and procedures will be addressed on the longer term, certain actions to improve law enforcement must be addressed as soon as possible considering the urgency to address issues about electronic evidence, considering further the ever evolving technologies and crimes. However, certain areas require further research before they can be addressed in the Common European Framework as there are too many uncertainties regarding these topics. Conducting further research is therefore an important objective that needs to be addressed as soon as possible for the results to be included within the Common European Framework.

18.4.1.1 Objective: Enhanced Law Enforcement

Most of the law enforcement challenges, which are plentiful, would primarily find a solution through legislative and/ or policy action. However, there are several actions that must be taken within the LEA community and the digital forensics community. An enhanced enforcement scheme should include many elements to address the law enforcement challenges. A number of these elements can be addressed on the short term by LEAs and law- and policymakers such as national governments and European institutions (Europol and Eurojust). This includes finding an interim solution for the MLA procedure in increased international cooperation and JITs, drafting and using SOPs to fill the gap between law and reality until such time when the law can be changed, as well as preparing the private sector for forensic readiness by building bridges across sectors and enhancing communication and transparency.

The current enforcement scheme leaves LEAs to operate in a field of patchwork legal solutions with many challenges. One of the most important challenges law enforcement is faced with is Mutual Legal Assistance (MLA). MLA procedures are not adapted to the realities of today's crimes, which are increasingly global, complex and fleeting and heavily impact the potential for rapid and efficient transfers of electronic evidence. Improving the MLA procedure on several levels is necessary. On a short term and as a transitional and complementary solution international coordinated investigations and joint investigation teams (JITs) should be further realised to deal with global and complex crimes before the MLA procedure can be digitised and on international law can be modernised, which will take longer to realise. More legal certainty and guidelines on international coordinated investigations and JITs are necessary. Apart from addressing the MLA procedure, other legal provisions and policies may also negatively impact investigations, for example, privacy and data protection laws, which may prevent the collection of evidence, and varied data retention periods across jurisdictions may complicate investigations. Legislation may furthermore not sufficiently address the realities of modern investigations, especially when it comes to evolving new technologies. This negative impact and lack of transparency increases scrutiny by civil society and creates a gap between stakeholders. It is therefore necessary that (1) LEAs, digital forensics and prosecution keep clear records of investigation procedures, (2) Standard Operating Procedures (SOPs) are drafted to bridge the gap between reality and legislation[11] and (3) communication and transparency are enhanced and bridges are built across sectors and between different stakeholders. The final challenge law

[11]Existing guidelines and best practices, such as the ENISA handbook and guide (ENISA, Identification and handling of electronic evidence—Handbook, document for teachers [2013] September 2013; ENISA, Electronic evidence—a basic guide for First Responders Good practice material for CERT first responders [2014]) and Council of Europe Electronic Evidence Guide (Council of Europe Data Protection and Cybercrime Division, Electronic Evidence Guide A basic guide for police officers, prosecutors and judges Version 1.0, Strasbourg France 18 March 2013, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic%20Evidence%20Guide/default_en.asp) may be used as a starting point to further

enforcement is faced with which may be solved on a short term is forensic readiness of the private sector. The importance of the private sector in criminal investigations is rapidly growing. The private sector has an impact on the development of new technologies, has more resources and electronic evidence may increasingly be held by the private sector (such as Internet Service Providers (ISPs)). To ensure correct handling of electronic evidence and enhance collaboration, the private sector should aim to reach an adequate level of 'forensic readiness' based on their activities and scale. This should be achieved by building bridges between the public and private sector and ultimately by clear legislation on a longer term. Preparing the private sector for 'forensic readiness' may be achieved by opening dialogue between stakeholders, by organising events and awareness raising campaigns across sectors on a European and international level.

18.4.1.2 Objective: Further Research

Many challenges to the current way of handling electronic evidence require further research before they can be included in the Common European Framework for electronic evidence. This includes some recent or modern developments, which have an impact on law enforcement and digital forensics in the collection and analysis of electronic evidence, such as crypto-currencies, Internet of Things and cloud computing. Developing research, techniques and software for the analysis of these developments is necessary to better understand the challenges and to provide clear and effective legal, policy, technical and other recommendations in this regard to include in the Common European Framework. It is furthermore necessary to identify how software technology can ease the capture of information to help verify admissibility criteria as the application of a technical solution can make electronic evidence become inadmissible and to improve investigative techniques, such as techniques for mobile devices and for data acquisition (including on mobile devices) before encryption, as well as possibilities for developing open source tools for specific acquisition. There is an abundance of best practices and guidelines concerning (electronic) evidence on a regional, national, European and international level. A lot of knowledge can be extracted from these best practices and guidelines to realise the Common European Framework in the best way possible.

Other challenges that would require further research are mainly legal challenges, such as constitutional limitations, data retention and the negative impact of legislation and policies on law enforcement. The systems of fundamental rights related to privacy and electronic data in the Member States are diverse resulting in constitutional limitations. Different constitutional traditions also lead to diverse implementation of international treaties such as the Cybercrime Convention. It is necessary to conduct an in-depth study to analyse the constitutional situation

build on. These SOPs should include record keeping and documentation by law enforcement, prosecution and digital forensics of the entire investigation process.

in the 28 Member States to allow for smooth implementation of the Common European Framework on the longer term. Data retention remains legal in some Member States despite the annulment of the data retention Directive by the Court of Justice of the European Union (CJEU). It is necessary to evaluate whether the remaining national provisions that had been implemented to transpose the annulled Directive and, which have not yet been removed, are possibly violating European fundamental rights and therefore must be annulled to evaluate which is the best way forward concerning data retention and safeguards thereof. Presently, data retention periods vary across jurisdictions. Harmonised legislation with appropriate safeguards in this regard is necessary. LEAs and prosecution should comment on the impact of data retention, the lack thereof in certain countries and the different periods applicable across countries from both a quantitative and qualitative perspective, as well as on other legislation and policies, which may negatively impact investigations. For example, privacy and data protection laws may prevent the collection of evidence and varied data retention periods across jurisdictions may complicate investigations. It is therefore necessary to collect feedback from LEAs and prosecution on the impact of certain laws, the severity of their impact and the frequency of their occurrence including the impact of data retention, the lack thereof in certain countries and the different periods applicable across countries from both a quantitative and qualitative perspective.

The areas for further research suggested in above have been selected based on the results of the EVIDENCE project and on what areas are most challenging for law enforcement and digital forensic specialists. However, there are more challenges that might be considered when realising the Common European Framework for electronic evidence, such as the dark net and malware. Concerning these topics, there is however already ample of research available and this was not seen as requiring most priority by the experts involved in the EVIDENCE project. The list of challenges and actions in this paragraph can therefore be seen as a non-exhaustive list of areas requiring further research or attention, notwithstanding any other relevant (technological) developments. It can furthermore be noted that, while further research in this document is indicated as a short-term solution, further research should always be an ongoing process, particularly considering the ever evolving technologies.

18.4.2 Medium-Term Solutions

Medium-term solutions address four objectives: enhanced legal provisions, enhanced exchange, enhanced trust and enhanced technical standards. Enhancing certain legal provisions that pose a challenge should be thought thoroughly and, as soon as possible, be addressed in the Common European Framework. To facilitate law enforcement and make investigations more efficient exchange should be enhanced as soon as possible. All actions cannot be addressed without the support of all actors and stakeholders involved. Trust issues should therefore be addressed

and action taken to enhance trust among actors. Electronic evidence cannot exist and the process cannot be facilitated without enhanced technical standards.

18.4.2.1 Objective: Enhanced Legal Provisions

There is a general lack of specific investigative measures. Not all methods sufficiently cover the specific nature of electronic evidence collection. For example, lawful interception, computer assisted search and seizure of electronic evidence are hardly regulated in specific terms across Europe. It is necessary to clarify what lawful interceptions are and how the use of potentially intrusive technologies are compatible with the rule of law to provide a clear legal basis for lawful interception bearing in mind modern technologies and preventing admissibility issues. Covert and remote measures particularly highly affect fundamental rights. It is necessary to implement clear and precise legal provisions with clear authority for LEAs, which includes adequate privacy safeguards addressing the privacy risks related to computer-assisted search, particularly covert and remote measures. While seizure is mostly regulated across Member States, there is a lack of specific legal provisions in seizure of data and data storage as opposed to seizure of physical objects. Seizure of data should only be legal if adequate safeguards are implemented. A data specific legal provision, which considers that seizure of a data carrier involves serious privacy risks, should make a distinction between seizure of data and seizure of physical objects with respect to the potential impact on fundamental human rights. All these elements and other investigative measures specific to electronic evidence should be regulated including legal safeguards. A more specific legal basis to collect electronic evidence is necessary, particularly to avoid admissibility issues in cross-border cases. A common European framework for the systematic and uniform application of new technologies in the collection, use and exchange of electronic evidence should thus include specific, clear and precise investigative measures in the collection of electronic evidence. Security, investigative and procedural measures must be proportionate and guided by core values such as human dignity, freedom, democracy, equality, the rule of law and the respect for fundamental rights. These specific investigative measures must be addressed to provide more clarity, legal certainty and authority for LEAs in certain areas. These legal provisions may be drafted or amended on a medium term to provide a legal basis and can be included in the enhanced legal framework on the longer term. Legislation and policies may negatively impact investigations. Based on the feedback collected from LEAs and prosecution on the impact of certain laws amendments to certain investigative measures should be discussed and proposed on a European and on a national level. SOPs should furthermore be drafted and adopted to fill the legislative gap. In this regard, existing guidelines and best practices, such as the ENISA handbook and

guide[12] and Council of Europe Electronic Evidence Guide[13] may be used as a starting point to further build on. This lack of a specific legal basis is furthermore challenging to the handling of electronic evidence considering that most Member States do not have a legal distinction between physical and electronic evidence. They apply traditional evidence rules to electronic evidence that, considering the specific nature of electronic evidence, may not be sufficient to cover electronic evidence. A distinction between physical and electronic evidence in legal provisions is recommended, or, where reasonable, the legal provisions should explicitly state that they apply to both physical and electronic evidence.

After the evidence has been collected, it needs to be preserved before it can be used in court. Preservation and storage of electronic evidence is of relevance, in terms of both implementation of adequate archival procedures of (long-term) preservation of electronic records that might one day become evidence, as well as proactive preservation of collected electronic evidence during the prosecution period (sometimes even a decade long). There is a general lack of legal provisions in the preservation of electronic evidence, including preservations methods and use, standards or guidelines on who is authorised to process the electronic evidence in what stage of the criminal proceeding, access restrictions, specifications on how the evidence must be preserved and stored and how to handle evidence obtained from private parties. It is necessary to introduce specific legal provisions concerning the preservation, storage and use of electronic evidence, including security measures and safeguards against alteration of data. Apart from legal provisions, it is advisable to draft operational guidelines, SOPs or similar in this regards. The Common European Framework needs to include legislative and other measures, including guidelines on the preservation and storage of electronic evidence, including rules on access restrictions, authorisation, method and duration of preservation, data protection, and other rules.

18.4.2.2 Objective: Enhanced Exchange

As previously stated, one of the most important challenges law enforcement is faced with is MLA considering that MLA procedures are not adapted to the realities of today's crimes, which are increasingly global, complex and fleeting and heavily impact the potential for rapid and efficient transfers of electronic evidence. Challenges in the MLA procedure must be addressed on multiple levels. After enhancing law enforcement by improving international cooperation and JITs on

[12]ENISA, Identification and handling of electronic evidence—Handbook, document for teachers [2013] September 2013; ENISA, Electronic evidence—a basic guide for First Responders Good practice material for CERT first responders [2014].

[13]Council of Europe Data Protection and Cybercrime Division, Electronic Evidence Guide A basic guide for police officers, prosecutors and judges Version 1.0, Strasbourg France 18 March 2013, available via: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic%20Evidence%20Guide/default_en.asp.

the short term this may be achieved in the second place and on a medium term by digitisation of the MLA procedure. Digitisation of requests and forwarding of evidence is necessary to address the challenge. e-MLA (Interpol), as well as solutions provided by the EVIDENCE project, are suggested as possible solutions in this regard.

18.4.2.3 Objective: Enhanced Trust

There is a general mistrust within the judiciary and other actors involved in the criminal trial, which includes fear of manipulation, vulnerability and misunderstanding concerning electronic evidence. Trust is necessary for all the other objectives to be successful. For the Common European Framework to be effective enhanced trust is necessary, particularly enhanced trust in the judiciary. It is not sufficient to enhance legislation, law enforcement and technical standards. Shared competencies and common values are necessary to support the ensemble of solutions proposed. Without cooperation of the actors involved the realisation of the Common European Framework will fail. The objectives and challenges proposed must be complemented by ethical and social action by addressing challenges such as mistrust, security, cultural differences, etc. to enhance trust among actors and trust in and within the judiciary. This can be achieved by (coordinated European) awareness raising activities, aimed at judiciary officials, magistrates and other actors involved in the criminal trial, as well as coordinated European meetings for actors in the field, to improve dialogue among actors to improve the general lack of communication, consensus and coordination between actors. Awareness raining campaigns should furthermore be aimed at the media and citizens. Media and citizens fail to understand the technical complexity and rapid technological developments and to consider the specificity of electronic evidence. Awareness raising activities and targeted training activities are required in this regard to improve cultural and personal oppositions and enhance trust.

Lack of trust also results from a lack of competences and professions. There is a general lack of technical knowledge, experience, education and training within the judiciary, as well as with prosecution and defence lawyers. It is a challenge to stay up to date with all the innovations and tools. It is desirable that every judicial actor is trained to guarantee minimum knowledge on electronic data and its use in the judicial system to reduce the waste of time and resources and to increase trust. This needs to be addressed by mandatory training (on technical issues, electronic evidence and digital forensics) of the judiciary in the field of electronic evidence. Coordinated European training programmes should be set up and carried out within the Member States to train judiciary officials within the field of electronic evidence. Compulsory education regarding these topics is furthermore necessary. These subjects should be added to the academic programme by consolidating them in the academic syllabus for legal studies to provide a basic knowledge of this by the judiciary. It is furthermore advisable to compile more information on the subject matter and develop a (cyber)crime repository including a repository of case law and lessons learnt.

Mistrust finally also results from a lack of competencies by certain (smaller) LEAs. Proper investigations require proper investigative tools. Mainly because of budgetary issues, not all LEAs possess proper investigative tools. This may impede trust in the evidence collected by (smaller) LEAs that do not have access to proper investigative tools. Investing in proper digital forensic tools is necessary. Particularly considering security challenges such as the volatile nature of data, difficulties to prove authenticity and possible manipulation, which make proper investigative tools a necessity for all LEAs.

18.4.2.4 Objective: Enhanced Technical Standards

An important part of the Common European Framework concerning the collection, preservation, use and exchange of electronic evidence includes enhancing technical standards. Technical action includes a proposed standard for representing data and metadata involved in the exchange process and formal languages for their representation. The EVIDENCE project provided a detailed overview on how to develop an electronic evidence exchange platform and introduced a cloud platform for implementing the exchange process, which includes features such as cryptographic control and malware protection and suggestions for the use of the evolving standards DFAX and CASE, that leverage the Unified Cyber Ontology. While some of the technical challenges may be addressed sooner than others, the general estimation is that enhancing technical standards will be addressed on a medium term.

One of the main technical challenges includes the lack of a standardised format and language, including the lack of a standardised format for representing the output of forensics analysis software, the lack of a standard format for information exchange, data and metadata processing, the use of a formal standard language for representing the wide range of digital forensic information and forensic processing results and a standard exchange method. The use of a common format and language (DFAX and its evolution called 'CASE' which is under development and should be considered) for exporting the metadata of the forensic investigation along with the associated findings will help transferring and comparing results between tools and thus assist verification of findings. A standard proposal for representing data and metadata involved in Electronic Evidence Exchange has been presented in Deliverable 4.1 of the EVIDENCE project that also recommends the use of DFAX, which later on ultimately evolved into CASE, for representing these metadata and describing in a detailed way all technical and legal forensic information. Previously, DFAX and the related formalisms were not mature enough, however, the design focuses on the extensibility and was therefore adaptable for covering all possible information needs for representing forensics investigations. The advantages of using such formalisms were clear:

- they have been developed in the cyber security environment but
- they include lots of essential elements to representing digital forensic information;

- they allow to describe technical, procedural and judicial information as well;
- they allow tools interoperability;
- they allow to compare results produced by different digital forensic tools;
- they leverage the UCO ontology that permits the description of Actions, Actors and their relationships within the Forensics Environment;
- they are open source;
- they already contain a composed structure for representing a wide range of forensic information.

The standard proposal chiefly consists of metadata and formalisms for their representation, so the platform on which these software layers may be implemented assumes less importance, while more relevant is the capacity/possibility to integrate this layers with an existing platform that is already up and running. All the platforms have already implemented security and privacy levels in accordance with standard ISO/IEC 27017, ISO/IEC 27002 and ISO/IEX 2704050 that guarantees a wide trust among all involved stakeholders.

The second technical challenge is due to the very nature of electronic evidence in that it is easier to copy or alter electronic evidence. Integrity checks when packaging and un-packaging the data and metadata using hash functions in this regard are necessary. These checks should be included in operational guidelines or SOPs. During the copying process, it is appropriate to carry out a hashing MD5 over the whole or parts of image to verify the integrity of the cloned data image. The most popular hashing function are those based on the MD5, SHA1 e SHA256 algorithms. It is crucial to have trustworthy data on which to carry out the analysis otherwise the analysis may have a limited or no value, since the evidence may be questioned during the trial. Each format allows to accomplish the acquisition task using a single file or splitting the copy into smaller pieces built up of many sequential files.

The acquisition can be accomplished using two distinct methods:

- dismounting the internal hard disk and then acquire the content using an external device (disk duplicator);
- using the personal computer itself, that contains the hard disk.

The first method is always recommended because it is less prone to making mistakes during the acquisition process, nevertheless there are cases where the second method is the only choice, such as in case of hard disks welded to the motherboard or computer hard to disassemble etc.

The acquisition based on the hard disk dismount is completed through the following steps:

- Usage of hardware duplicator or disk imaging tools;
- Usage of a forensics workstation with acquisition forensic tools using:
  - a write blocker hardware or;
  - a write blocker software.

Integrity checks when packaging and un-packaging data must be introduced and included in SOPs.

Mobile devices pose a particular challenge as acquisition entails various risks including tangling with the integrity of the original source of evidence. Evidence acquisition has some risks for the device state preservation. Unlike other storage device acquisition where the memory can be detached from the device and acquired afterwards using technologies described in previous sections, the mobile device acquisition requires the interaction with the device, the use of the installed operating system and the related communication protocols through a computer or directly loading an alternative operating system into the RAM (i.e. an injection technique). Special action should be taken to prevent from triggering security systems that might put the data integrity at risk. The Guidelines on Mobile Device Forensics (NIST Guidelines on mobile device forensics, 2014) should be used and constantly updated and delivered to LEAs in a concise format for facilitating their interventions/ tasks at least for the most common mobile devices. It would furthermore be desirable to develop a specific App for mobile devices as a first guide to carry out the initial forensic tasks. Based on the mobile device, model is necessary to take special care during the device interaction to prevent from trigging security systems that might put at risk the data integrity (i.e. erase all data on this iPhone after ten failed passcode attempts). Possibilities for this App should be investigated on the short term. Action includes using, constantly updating and delivering the guidelines on mobile device forensics (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf) to LEAs in a concise format for facilitating interventions/ tasks for mobile devices and develop a specific application for mobile devices as a first guide to carry out the initial forensic tasks.

Exchange of electronic evidence is of the utmost importance, particularly in cross-border cases. The efficiency of data exchange relates to the amount of resources expended including time in relation to the accuracy and completeness with which users exchange data holding or potentially holding electronic evidence. A standard exchange method is necessary. Standard methodology, structure and formatting of evidence data analysis and exchange methods will help efficiency. The trust of data exchange relates not only to the ability to guarantee a reliable data exchange means between well identified stakeholders with proper authorisation but also on the ability to obtain a complete provenance of data received from the authentic electronic source including the chain of custody and the tools used to collect, extract and analyse data up to the data received by a recipient of the exchange. The EVIDENCE App and DFAX language implement these features by design. It is necessary to introduce a standard exchange method and language, the EVIDENCE application and DFAX and CASE language are recommended. An electronic evidence exchange system must furthermore reliably keep information confidential and respect data protection policies while, at the same time provide a means to verify the authentic origin of the data. Encryption of identities and sensitive private data of persons involved in the case or working on it is suggested, as well as

security of investigation information by encryption of packages.[14] The EVIDENCE Application should be integrated with the user management system and deployed within a secure environment and privacy guidelines should be drafted in this regard. Policies and guidelines for information security should guarantee the protection of all assets involved in the exchange process information flow to create trust to all potential stakeholders/users. There is no uniform evidence exchange platform, it is recommended to establish an Evidence Exchange Platform. A general architecture of the cloud platform is necessary where there is a sender and a receiving authority who will be authenticated and authorised to upload/download data and meta data, relying on trusted mechanism, allowing to share data across different countries/jurisdictions and considering privacy/security issues. The platform should include:

- Access control;
- Physical and environment security;
- Backup;
- Malware protection;
- Cryptographic control;
- Communication security;
- Personal data and privacy protection.

Exchange of analysis results is sometimes difficult because it highly depends on the type of object to describe as Output. There are certain issues that must be addressed and extended in DFAX (standard)/CybOX formalism, including:

- The lack of Cybox objects to describe most of the common artefacts extracted from a source of evidence/ acquisition;
- Correlation between the extracted information and the tool used to recover/interpret it (e.g. specific tool used to recover internet history);
- Relationship between objects that share the same characteristics (e.g. two identical files, same MD5 hash, that are stored in two different Devices);
- There is no way to describe deleted contents (i.e. files or records within the unallocated space of a device);
- There is a need to describe general objects, such entry in a SQLite database.

Issues with the DFAX structure and its expansion in exchange languages include:

- The case information part of the DFAX Package is structured with a strict authority–investigator–victim–subject paradigm. This fields must be discussed with legal experts for establishing if they fit into reality, also bearing in mind the different law systems existing among European countries and the rest of the world.

[14]Data markings are an integral component of CASE (see Chap. 4), permitting information to be labeled as private or sensitive, and to be shared or protected appropriately at different levels of trust and classification. UCO provides for data markings that CASE can use to support proper handling of shared information (http://legacydirs.umiacs.umd.edu/~oard/desi7/papers/EC.pdf).

Table 18.1 Objects to be added to DFAX standard

Object	References
Windows Jumplist	Like shortcuts files it is commonly used to identify file access
Windows Shortcuts	It is an artefact commonly used during forensic investigation to identify file access, device connection, network shares, and so on. It should be described by its specific fields
Windows Prefetch	It is an already existing Object in Cybox but its structure has changed since Windows 8, so the object needs to be updated
Office Document	Useful for describing Office Documents in terms of metadata
Image File	Already existing object in Cybox. It should be updated to describe typical image metadata
Audio File	Same concept as an Image file applied to an Audio
Video File	Same concept as an Image file applied to a Video
Database Entry	Generic way to describe database entry in a table or the result of a SQLite query
Generic artefacts	Record/data contained inside a file in proprietary format. For example, an entry contained in a chat or P2P history file (i.e. MET files used by eMule software) or a plist file used in Apple OS for configuration and data
PCAP File	It should be useful to have a way to describe a Network Capture file with some metadata, for example those extracted by tools like capinfos; See the Catalogue at wp4.evidenceproject.eu)
Deleted Files	There should be a way to describe deleted files

- The use of a specification such as CybOX is useful in a Digital Forensic context is necessary to define a list of common terms to be used for describing objects. For example:
  - Device object is commonly used to describe physical source of evidence and should contain a description field. Examples of fixed description values could be: Personal Computer, Notebook, SATA Hard Disk, USB Hard Disk, USB Pen Drive, CD, DVD, SD Memory Card, Smartphone, Tablet, etc.;
  - Some physical objects may contain specific fields that must be defined. For example, in the case of a smartphone, it is more appropriate to use the IMEI rather than a serial number value.

It must be mentioned, however, that these issues and limitations were addressed when DFAX evolved into CASE, as discussed in Chap. 2.

Table 18.1 shows the changes that must be made to CybOX.

18.4.3 Long-Term Solutions

Long-term solutions address four objectives: enhanced legal framework, enhanced policies, enhanced law enforcement and professionalisation in the field of digital forensics. By addressing the actions in this paragraph all previous objectives will

come together, will be finalised and the Common European Framework will be realised. Law and policies will be modernised and law enforcement facilitated.

18.4.3.1 Objective: Enhanced Legal Framework

There is a legislative gap concerning the collection, preservation, use and exchange of electronic evidence considering that there is no comprehensive legal framework and no legislative harmonisation. There is a patchwork of legislation, implemented differently among Member States causing legal and practical uncertainty. Existing legislative and enforcement frameworks and the concepts enshrined therein, as well as data protection concepts, precede the creation of the internet as we know today and do not satisfactory deal with the realities of technological developments and with the dynamic nature of modern investigations. There is no uniform definition of electronic evidence and a lack of a comprehensive European legal framework addressing data protection issues related to electronic evidence. The legislative gap leaves LEAs to operate in a field of patchwork solutions and playing catch up and manoeuvering their way through a highly uncertain and politically sensitive landscape filled with legal lacunae. Suggestions can be made for modernising and harmonising legislation and policy, including international law and treaties and for operational guidelines and SOPs as standards on the procedures and modalities to follow in the phase of collection, preservation and exchange of electronic evidence, which ensure proportionality between protection of privacy and infringements for legitimate crime prevention and control.

Legal challenges mostly originate from the fact that criminal law is mainly regulated at national level. This is challenging considering that all Member States have different rules, procedures and approach, making cross-border cooperation challenging in this modern society filled with evolving technologies. Uniform European standards would aid investigations in criminal cases and facilitate the process of exchange. A Common European Framework for the systematic and uniform application of new technologies in the collection, preservation, use and exchange of electronic evidence should be based on clear and specific rules for the collection of electronic evidence, common definitions and standards and approximation of legal procedures. There is a general lack of uniform European standards, particularly about:

- Uniform definitions;
- Uniform definition of electronic evidence;
- Standards for information exchange;
- Lack of communication/ agreement/ coordination between actors and difficulties in sharing information (between offices and organisations);
- Procedures and guidelines for the collection, preservation and use of electronic evidence;
- Procedures for the validation of electronic evidence;
- Methodologies for analysis;
- Technical infrastructure.

Lack of such standards causes difficulties on multiple levels including delays in obtaining and interpreting electronic evidence, admissibility, etc. This needs to be addressed on multiple levels to achieve the Common European Framework. Standardisation of procedures and drafting and disseminating guidelines is required. Practices should be disseminated and mainstreamed, partnership should be built (public, private, research, civil society) and coordinated European training and certification should be organised to improve the lack of uniform European standards from an ethical and social perspective to enhance trust. Trust should be enhanced by education, training and awareness raising campaigns, bridges should be built across sectors and technical solutions must be provided. While most of the uniform standards will be addressed from multiple angles, it is necessary to have a legal structure complemented by SOPs in the operational guidelines or rules on the actual handling of electronic evidence. While all Member States have within their country certain specific agencies or units, particularly forensic institutes, specialised in the collection, examination and preservation of evidence, there are limited guidelines or procedures for the use of digital technologies in criminal proceedings. A common European framework for the systematic and uniform application of new technologies in the collection, use and exchange of electronic evidence should thus include a plan for the development of common guidelines and procedures.

Legal challenges also originate from the fact that legislation lags behind rapidly developing technologies. Existing legislative and enforcement frameworks and data protection concepts do not satisfactory deal with the realities of technological developments. Legislation should be technology neutral and include new or adapted investigative measures. General laws may not provide solutions for today's digital society. Analogous argumentation of traditional legislation may not suffice and may not provide sufficient safeguards against potential privacy infringements. IoT, virtual currencies and other new developments and technologies present new challenges for LEAs, forensic analysts and the procedures, methods and tools they apply. Risks include disproportionate collection, misuse and transfer. Modernising and harmonising legislation and policy including authorisation for the collection of electronic evidence accompanied by specific safeguards to mitigate the impacts on fundamental rights and new/ adapted investigative measures is required. The legislative gap should be addressed by legislation that is fit-for-purpose with appropriate safeguards. From a EU perspective, existing legislation such as the European Investigations Order Directive[15] may be taken as a starting point to build further on and implement measures further to address the specificity of electronic evidence. Drafting and adopting fit-for-purpose legal provisions addressing the technological challenges while maintaining appropriate safeguards is of the utmost importance.

These fit-for-purpose legal provisions should include specific investigative measures considering that not all measures sufficiently cover the specific nature of

[15]Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters [2014] OJ L 130/1.

electronic evidence collection. Certain interception and search and seizure methods (that lead to electronic evidence) are not sufficiently covered legally. Where rules exist these follow from the provisions of the Cybercrime Convention and apply mostly to the investigation of cybercrimes. Most of the Member States extend the application of traditional investigative methods to electronic evidence. While in some cases this might work, generally, these methods do not sufficiently cover the specific nature of electronic evidence collection. A more specific legal basis is necessary to obtain electronic evidence, particularly to avoid admissibility issues in cross-border cases. A common European framework for the systematic and uniform application of new technologies in the collection, use and exchange of electronic evidence should thus include specific, clear and precise investigative measures in the collection of electronic evidence. One of the main gaps in investigative powers includes the lack of power to enter electronic networks to search for evidence and to preserve computer data to support existing search powers. Legislation requires a clear scope of application of powers and sufficient legal authority for action accompanied by specific safeguards. A more specific legal basis is necessary to obtain electronic evidence, particularly to avoid admissibility issues in cross-border cases. A common European framework for the systematic and uniform application of new technologies in the collection, preservation, use and exchange of electronic evidence should thus include specific, clear and precise investigative measures in the collection of electronic evidence. Security, investigative and procedural measures must be proportionate and guided by core values such as human dignity, freedom, democracy, equality, the rule of law and the respect for fundamental rights. One of the specific challenges in investigative measures is posed by cloud computing. There is a general lack of legal basis in Europe regarding investigation in the cloud. The Common European Framework should include specific provisions in the collection of electronic evidence out of a cloud service. This rule should go further than the search and seizure rules (for electronic evidence) that exist in the Cybercrime Convention, particularly as the current rules are bound to the territorial jurisdiction of the state where the investigation is taking place. Rules on the obtaining of evidence from the cloud need to go beyond the current limitations of territorial jurisdiction. One possible way is to agree on a 'universal jurisdiction' approach particularly in the investigation of serious crimes (here too however, the term 'serious crimes' may need to be defined further). Data is distributed to storage locations that in some occasions can be unknown, which may lead to jurisdiction issues such as overlapping jurisdiction. Another jurisdiction approach is an investigative jurisdiction based on a legitimate interest. Certain legal developments and studies should be considered while drafting the enhanced legal framework. A legal basis for investigations in the cloud is necessary including harmonised privacy safeguards for the collection of electronic evidence out of cloud storages. Based on the recommendations provided by further research in this regard investigations in the cloud should be regulated in the Common European Framework.

Considering modern technological developments, which have a changed impact on fundamental rights and the unchanged rules and safeguards to protect such rights, it is necessary for the Common European Framework for electronic evidence to

consider the changed impact and to provide sufficient safeguards. All Member States have at least one important basis in common: protection of fundamental rights. The collection, preservation, use and exchange of electronic evidence can only be sound and effective if it is based on fundamental rights and freedoms and individuals' rights cannot be secured without safe networks and systems. Law enforcement, prosecution and the judiciary should execute investigative powers and procedures with regard for human rights and liberties. Protecting fundamental rights, freedom of expression, personal data and privacy are of utmost importance. Therefore, security, investigative and procedural measures must be proportionate and guided by core values such as human dignity, freedom, democracy, equality, the rule of law and the respect for fundamental rights. Fundamental rights, democracy and the rule of law must be protected in cyberspace while protecting against incidents, malicious activities and misuse. These rights and freedoms also include the right to a fair trial, particularly when preparing a defence case where electronic evidence forms part of the evidence. All respondent Member States provide for the codification of fundamental rights. Any common European framework for the systematic and uniform application of new technologies in the collection, use and exchange of electronic evidence should be based on the protection of fundamental rights and freedoms, including proper restrictions and safeguards. The basis for this already exists in the Member States of the EU through the ratification of the ECHR and through constitutional provisions and traditions in the different Member States. Data protection concepts precede the creation of the internet as we know today and do not satisfactory deal with the realities of technological developments. The enhanced legal framework should respect fundamental rights, include a minimum standard of data protection, privacy safeguards, security standards and should be accompanied by operational guidelines and rules on the handling of electronic evidence. Action includes drafting and adopting legal provisions, which respect fundamental rights, data protection standards, privacy safeguards and security and ensure that the entire Common European Framework respects such principles and values.

One of the major legal challenges to be addressed is data collected by the private sector. The importance of the private sector concerning criminal investigations is rapidly growing that creates a dependency of LEAs on the private sector for the collection, examination, preservation and transfer of electronic evidence. The private sector has an impact on the development of new technologies, has more resources, digital forensics expertise is more common in the private sector than in the public sector and electronic evidence is increasingly being captured and held by the private sector (ISPs). A large part of electronic evidence originates from private sector actors, e.g. ISPs providing traffic data of internet transactions, telecommunications providers providing information on mobile communications, etc. Legislation does not clearly regulate the relationship with the private sector. It is necessary to have clear rules of what categories of data can be obtained from the private sector and what procedures need to be followed, i.e. the origin, collection and use of electronic evidence from the private sector and transfer of evidence from the private sector to LEAs. Regulation in the transfer of electronic evidence between LEAs and the private sector including safeguards in the development stages of new

technologies must be put in place. This should include a standard (secured) format for delivering data to LEAs from private sector is necessary to facilitate and speed up investigations. Challenges with connected devices and IoT include issues such as transfer of data from private to public sector, sensitive data and big data. A major problem of obtaining electronic evidence from ISPs is represented by the growing world of services on mobile devices, based on apps. In theory every app producer can be a service provider, but at the same time not be viewed legally as such, meaning that they do not have the corresponding legal duties making investigations challenging. Privacy by default and focus on the quality of the information (instead of data overload) are recommended in this regard. Clear rules in the transfer from the private to the public sector are necessary, as well as training the private sector for 'forensic readiness'. To ensure correct handling of electronic evidence and enhance collaboration, the private sector should aim to reach an adequate level of 'forensic readiness' based on their activities and scale. The Common European Framework needs to include rules on the engagement of private sector experts and on how electronic evidence is transferred to and from private sector experts.

The second major challenge is data collected by SIS or actionable intelligence. Transfer of information or actionable intelligence between intelligence agencies and LEAs and vice-versa is often not regulated. The distinction in legal treatment (and application of laws) to law enforcement and security services/ intelligence agencies is not always clear. In most cases, the prime function SIS is to produce actionable intelligence that is passed on to the LEAs to act, whether it is to further monitor, follow, detain, arrest or prosecute a person or group of persons. It is therefore necessary to include in a common European framework for electronic evidence rules on the transfer and exchange of information/actionable intelligence and whether this information can be admitted as evidence in a criminal trial. Rules in this regard are necessary to establish whether the information or actionable intelligence can be admitted as evidence in a criminal trial. If the origin of the data is unknown or if the data was collected by SIS, the legitimacy of the source and transfer might be put in question as a clear chain of custody and documentation thereof is missing. It is suggested to introduce a pseudonymisation process, to develop and establish internationally agreed standards with an interdisciplinary approach, to flag the unknown origin for transparency and to enable to use appropriate analysis techniques. Legal provisions about data collected by SIS must be drafted and adopted.

The final major challenge is exchange of electronic evidence. There is a general lack of regulation in the transfer and exchange of electronic evidence, within domestic boundaries and internationally. Most of the rules that exist nationally, if any, have been prepared by some of the prominent actors themselves, e.g. most national forensic institutes have rules on the receipt and transfer of electronic evidence to be examined by them. Considering the volatile nature of electronic evidence and the large potential of tampering with the evidence during electronic evidence's lifecycle, which could lead to the inadmissibility of the evidence and/ or affect the fundamental rights of suspects and/ or victims, clear rules in this regard are necessary. Internationally speaking, it is increasingly evident that (apart from

the provision of the Cybercrime Convention) the procedures offered in existing legal frameworks are too slow for the volatile and fast-moving nature of electronic evidence. The provisions and procedures in the Cybercrime Convention are better suited for electronic evidence but States have often not extended their application beyond the scope of the Cybercrime Convention when ratifying the Convention. Clear rules in the transfer and exchange are necessary and can be built on the existing provisions and procedures in the Cybercrime Convention and on the current efforts of the Council of Europe to create an electronic version of the mutual legal assistance request form. Legal provisions concerning transfer and exchange of electronic evidence, particularly in cross-border cases, must be drafted and adopted. Considering that MLA procedures are not adapted to the realities of today's crimes that are increasingly global, complex and fleeting and that they heavily impact the potential for rapid and efficient transfers of electronic evidence it is necessary to increase international coordinated investigations. Under the auspices of Europol and Eurojust several JITs have been set up during investigations. These joint investigations allow for an efficient way of collecting and sharing of electronic evidence pertinent in an investigation. The common European framework should increase the legal certainty needed for such joint investigations to be carried out in a smoother and more efficient manner building on Council Framework Decision 2002/465/JHA.[16] Legal provisions increasing the legal certainty of JITs must be drafted and adopted. Considering that MLA procedures are not adapted to the realities of today's crimes that are increasingly global, complex and fleeting and that they heavily impact the potential for rapid and efficient transfers of electronic evidence it is necessary to digitise the MLA procedure and to provide a legal basis in this regard. Concerning the MLA procedure, it is furthermore necessary to eventually modernise international law. The legislative gap should be addressed by modernising and harmonising legislation and policy, including international law and treaties and adapting it to new technologies. A sound legal basis including uniform definitions (including a definition of electronic evidence), concepts and standards, access to investigative tools and techniques, training and technical capabilities, best practices policies that ensure proportionality between protection of privacy and infringements for legitimate crime prevention and control, and will facilitate a more efficient cooperation is required. Existing international law, such as the Cybercrime Convention[17] and the European Convention on mutual assistance in criminal matters[18] may be further build upon to address the challenges law enforcement is faced with when dealing with electronic evidence. Possibilities for modernising international law including draft amendments, new laws and recommendations

[16]Council Framework Decision of 13 June 2002 on joint investigation teams (2002/465/JHA) [2002] OJ L 162/1.

[17]Convention on Cybercrime [2001] ETS 185.

[18]European Convention on Mutual Assistance in Criminal Matters [1959] CETS 030; Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters [1978] CETS 099.

should be discussed by the Council of Europe, the EU, LEAs, digital forensics, lawyers, private sector, national governments and European institutions.

18.4.3.2 Objective: Enhanced Policies

Challenges to the collection, preservation, use and exchange of electronic evidence cannot be addressed without clear policies reflecting the objectives to enhance legislation, law enforcement, trust and technical standards. Modernised policies should be aimed at enhancing legislation, investigation, prosecution, enforcement, trust and technical standards. These policies should support international cooperation, reflect the realities of new crimes, new technologies and new investigations and should ensure proportionality between protection of privacy and infringements for legitimate crime prevention and control and be guided by core values such as human dignity, freedom, democracy, equality, the rule of law and the respect for fundamental rights.

18.4.3.3 Objective: Enhanced Law Enforcement

LEAs are left to operate in a field of patchwork solutions and playing catch up and manoeuvering their way through a highly uncertain and politically sensitive landscape filled with legal lacunae. Most of the law enforcement challenges, which are plentiful, would primarily find a solution through legislative and/ or policy action. However, there are several actions that can be taken within the LEA community and the digital forensics community. An enhanced enforcement scheme should include many elements to address the law enforcement challenges. This includes investing in tools and training for LEAs. Modern crimes need modern solutions. LEAs cannot afford to lag behind innovations considering that criminals have access to modern tools and techniques. Enhanced enforcement requires access to investigative tools and techniques, training and technical capabilities. Access varies among LEAs, particularly mainly because of budget issues. For the system to be effective all LEAs should have similar access to tools, techniques, training and technical capabilities.

One of the law enforcement challenges is issues with law enforcement databases including purpose limitation, big data and interoperability. It is necessary to restrict the use to severe crime only and to introduce a life-cycle control of data, which is case independent. It is furthermore necessary to regulate and establish a gateway for interoperable standard interchange based upon open and existing standards and controls at EU level and international level. Preservation of electronic evidence is of relevance, in terms of both implementation of adequate archival procedures of (long-term) preservation of electronic records that might one day become evidence, as well as proactive preservation of collected electronic evidence during the prosecution period (sometimes even a decade long). There is a lack of standards for storage that should be addressed. It is necessary to introduce a case independent data life-cycle

control and a gateway for interoperable standard interchange and draft guidelines for preservation and storage.

Considering the volatile nature of electronic evidence and to prevent admissibility issues it is necessary to follow uniform guidelines on the handling of electronic evidence, preservation thereof, methods and use, as well as access control and restrictions. Enhanced enforcement should include standards or guidelines on who is authorised to process the electronic evidence, in what stage of the criminal proceeding and should restrict access and provide specifications on how the evidence must be stored, preserved and should include guidelines on how to handle evidence obtained from private parties. Draft SOPs on handling electronic evidence are necessary. Existing guidelines and best practices, such as the ENISA handbook and guide[19] and Council of Europe Electronic Evidence Guide[20] may be used as a starting point to further build on.

18.4.3.4 Objective: Professionalisation in the Field of Digital Forensics

Most of the law enforcement challenges, which are plentiful, would primarily find a solution through policy and/ or legislative action. Part of these challenges may be addressed by professionalisation in the field of digital forensics. Professionalisation in the sub-discipline of digital forensics is necessary to achieve a certain level of professionalism and recognition within this young field. This requires standardisation efforts, reassessing potential regulation of digital forensics professions to ensure that practitioners meet a certain standard, validation of tool to ensure they are fit-for-purpose and accreditation for digital forensic labs to ensure that they meet certain pre-determined quality levels. Professionalisation in the field of digital forensics will complement law enforcement and includes regulation and certification of the profession and training, validation of digital forensic tools and accreditation of digital forensics labs.

The digital forensics profession is generally considered to be vague. There is a lack of certification models and specialised judicial services, high cost of examining and interpreting information, lack of expertise of the judiciary, difficulties related to the non-binding nature of international cooperation, jurisdiction issues and insufficient involvement of justice operators in the implementation of software. This can be addressed by recognition of the social and economic status of experts in the field of electronic evidence, introducing common certification, enhancement and coordination of expertise, involvement of internet governance bodies, coordination

[19]ENISA, Identification and handling of electronic evidence—Handbook, document for teachers [2013] September 2013; ENISA, Electronic evidence—a basic guide for First Responders Good practice material for CERT first responders [2014].

[20]Council of Europe Data Protection and Cybercrime Division, Electronic Evidence Guide A basic guide for police officers, prosecutors and judges Version 1.0, Strasbourg France 18 March 2013, available via: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic%20Evidence%20Guide/default_en.asp>.

of LEAs, overcoming difficulties between LEAs and service providers (by speeding up the process for accessing data in another jurisdiction, evaluating proportionality of requests, standardised electronic requests in agreement with providers, etc.). It is necessary to develop a system for coordinated European certification of digital forensic professionals and an official registry to provide for recognition of experts. To achieve a certain level of professionalisation degrees and certification for digital forensic professionals are necessary to ensure practitioners meet a certain standard (minimum degree and certification of digital forensic professionals by an independent certification board or organisation). A register of court experts at European level should be created that guarantees the quality of the contribution made by court experts to the legal process. It is essential to create a digital forensics experts register valid at European level. This would guarantee the quality of the professional advice, make the investigation faster, ensure the rights of the defence, foster the investigation of the public prosecutor and avoid questioning during the debate in front of the court.

There is an abundance of digital forensic tools, which vary in quality. LEAs and digital forensic professionals should work with the best available tools. Considering the large number of available tools on the market it is necessary to validate and certificate digital forensic tools, and/or validation of specific features of these tools to determine if a tool is legitimate to use during an investigation. Certification for tools is required to determine if a tool is legitimate to use during investigation. It is necessary to subject tools to validation procedures and to introduce certification. It is furthermore necessary to document what process was followed during the collection of electronic evidence, i.e. require proper documentation of what process was followed during the evidence gathering. Digital forensic tools require rigorous testing prior to use to catch bugs before they negatively impact a digital investigation. Some such datasets have been made available, including the Digital Forensic Tool Testing (DFTT) project, the NIST Computer Forensic Reference Data Sets (CFReDS) and the Digital Corpora project. Certification for tools is required to determine if a tool is legitimate to use during investigation or introduce a process certification, requiring proper documentation of what process was followed during the collection of electronic evidence. Each test must be accompanied by the following information:

- author of the test;
- date of the test;
- aim of the test;
- expected findings;
- equipment used to perform the test.

Test results must be repeatable and reproducible to be considered reliable from a scientific point of view. Digital forensics test results are repeatable when it is possible to get the same results using the same methods and starting from the same testing framework. Dual-method, or dual-tool, verification is the practice of using more than one method to verify data extracted. In doing so, a comparison is made between the two data sets to conclude the accuracy and precision of the data. While this practice may seem advantageous to determine the quality of evidence,

there are also a few main limitations, as discussed in the following points. Dual-method, or dual-tool verification is not a substitute for method validation. It may allow further confidence in evidence obtained via either method, but only if they are known to operate independently of one another. Method validation on both tools should be conducted if possible. Validation and certification of digital forensic tools and process documentation during the collection of electronic evidence is necessary. The tools catalogue developed by the EVIDENCE project can be used as a system for the validation of tools.

There is a limited recognition for the digital forensics profession that includes a lack of standardised training. Professionalisation on international, national and regional level is required. Effective police and judicial cooperation requires broader, international and regional standardisation efforts. Therefore, the establishment of regional Forensic Science Regulators would be recommended, particularly a European Forensic Science Regulator. Standardisation should refrain from hampering innovation and advances and should involve all stakeholders. Training should include updated knowledge investigations of cloud environments and mobile devices. National Forensic Science Regulators and an overarching European Forensic Science Regulator to standardise training of digital forensic professionals should be established.

To achieve a certain level of professionalisation within the field of digital forensics it is necessary to provide for accreditation of digital forensics labs. Accreditation will address standardisation and professionalisation of current practices and ensure that labs and the processes they implement meet certain pre-determined quality levels. Furthermore, new standards that are more applicable to forensic science in general and/or convert existing ISO/IEC guidelines on digital forensics into standards are also suggested to further professionalise the field. Standards and procedures for accreditation of digital forensic labs should be established.

18.5 Conclusion

In the digitalised world we live in there is an increase in the use of electronic evidence in criminal proceedings. Evidence in criminal cases is collected by enforcement authorities, preserved and used in criminal proceedings and possibly exchanged (cross-border) between authorities. To effectively prosecute crimes, law enforcement authorities must adapt to rapidly developing technologies by working with electronic evidence generated by these new technologies and by using digital technologies themselves to collect evidence. There is no comprehensive EU legal framework regarding electronic evidence and law enforcement is left to operate in a patchwork of solutions. Existing legislative and enforcement frameworks and the concepts enshrined therein, as well as data protection concepts precede the creation of the internet as we know today and do not satisfactorily deal with the realities of technological developments. Considering the very nature of electronic evidence and rapidly evolving technologies and crimes it is important to act now and to

address the challenges within the current system by realising a Common European Framework for the collection, preservation, use and exchange of electronic evidence to improve the efficiency of investigations and judicial procedures while maintaining adequate safeguards aimed at protecting relevant fundamental human rights and respecting clear standards of conduct.

These challenges must be addressed to reach the following objectives:

- **Objective 1: Enhanced law enforcement**;
- **Objective 2: Further research**;
- **Objective 3: Enhanced legal provisions**;
- **Objective 4: Enhanced exchange**;
- **Objective 5: Enhanced trust**;
- **Objective 6: Enhanced technical standards**;
- **Objective 7: Enhanced legal framework**;
- **Objective 8: Enhanced policies**;
- **Objective 9: Enhanced law enforcement**;
- **Objective 10: Professionalisation in the field of digital forensics**.

To reach these objectives, actions should be taken on a short, medium or long term that must be taken together for changes to the current system of handling electronic evidence to be more effective.

The **short-term solutions** address two objectives: enhanced law enforcement and further research. Enhancing law enforcement is the major objective of this Roadmap considering that LEAs are the most important actors involved with electronic evidence. Law enforcement needs to work with the rules and procedures provided to them by law- and policymakers. Most of the law enforcement challenges, which are plentiful, would primarily find a solution through legislative and/ or policy action. However, there are also other measures that can be taken to enhance law enforcement. This includes improving the MLA procedure on a short term by enhancing international coordinated investigations and joint investigation teams (JITs). It furthermore includes addressing the negative impact of legislation and lack of transparency by keeping clear records of investigation procedures, drafting SOPs which bridge the gap between reality and legislation and by building bridges across sectors, particularly between the public and private sector by achieving an adequate level of 'forensic readiness' of the private sector.

Certain areas require further research before they can be addressed in the Common European Framework as there are too many uncertainties regarding these topics. A better understanding of these challenges is necessary to provide clear and effective legal, policy, technical and other recommendations, which can be included in the Common European Framework. This includes research concerning constitutional limitations, data retention, the negative impact of legislation, crypto-currencies, the Internet of Things, cloud computing, technical solutions for admissibility, improving investigative techniques and best practices.

The **medium-term solutions** address four objectives: enhanced legal provisions, enhanced exchange, enhanced trust and enhanced technical standards. Enhancing certain legal provisions, particularly investigative measures, which pose a challenge,

should be addressed as soon as possible for these legal provisions to be taken forward in the Common European Framework. There is a general lack of specific investigative measures and not all methods sufficiently cover the specific nature of electronic evidence collection. A more specific legal basis to collect electronic evidence is necessary, particularly to avoid admissibility issues in cross-border cases. A common European framework for the systematic and uniform application of new technologies in the collection, use and exchange of electronic evidence should thus include specific, clear and precise investigative measures in the collection of electronic evidence. This includes a legal distinction between physical and electronic evidence, lawful interception, computer-assisted search, seizure and preservation and storage. These specific investigative measures must be addressed to provide more clarity, legal certainty and authority for LEAs in certain areas. The provisions may be drafted or amended on a medium term to provide a legal basis and can be included in the enhanced legal framework on the longer term.

To facilitate law enforcement and make investigations more efficient exchange should be enhanced as soon as possible. MLA procedures are not adapted to the realities of today's crimes that are increasingly global, complex and fleeting and heavily impact the potential for rapid and efficient transfers of electronic evidence. Digitisation of the MLA procedure (request and forwarding of evidence) is necessary to address the challenge. Solutions provided by e-MLA, as well as the EVIDENCE project are recommended in this regard.

All actions cannot be addressed without the support of all actors and stakeholders involved. It is not sufficient to enhance legislation, law enforcement and technical standards. For the Common European Framework to be effective enhanced trust is necessary, particularly enhanced trust in the judiciary. Ethical and social issues should therefore be addressed and acted upon to enhance trust among actors, for example, by awareness raising aimed at the judiciary and aimed at the media and citizens and by improving dialogue among actors. This should be complemented by addressing the lack of technical knowledge, experience and training within the judiciary by coordinated European training programmes and improved education.

An important part of the Common European Framework includes enhancing technical standards. Technical action includes a proposed standard for representing data and metadata involved in the exchange process and formal languages for their representation, a Digital Forensic Tools Catalogue, introduction of a cloud platform for implementing the exchange process and a Proof of Concept application on the electronic evidence exchange, persistence and support for maintaining a detailed chain of custody. These technical solutions should address the technical challenges identified in this Roadmap to improve the efficiency of investigations and exchange.

The **long-term solutions** address four objectives: enhanced legal framework, enhanced policies, enhanced law enforcement and professionalisation in the field of digital forensics. By addressing the long-term solutions all previous objectives will come together and finalise the Common European Framework. Law and policies will be modernised and law enforcement facilitated.

The enhanced legal framework should address the legislative gap concerning the collection, preservation, use and exchange of electronic evidence. Existing

legislative and enforcement frameworks and the concepts enshrined therein, as well as data protection concepts, precede the creation of the internet as we know today and do not satisfactory deal with the realities of technological developments and with the dynamic nature of modern investigations. The Roadmap provides actions for modernising and harmonising legislation and policy, including international law and treaties and for operational guidelines and SOPs as standards on the procedures and modalities to follow in the phase of collection, preservation and exchange of electronic evidence, which ensure proportionality between protection of privacy and infringements for legitimate crime prevention and control. This includes action as regards data collected by the private sector by further building on the forensic readiness of the private sector, building bridges and improving dialogue across sectors as well as drafting and adopting clear rules as regards transfer of data from the private sector and handling of electronic evidence by the private sector and regulation of a standard (secured) format for delivering data to LEAs from the private sector to enhance cooperation between the public and private sector. It also includes addressing the lack of uniform European standards to aid investigations in criminal cases and facilitate the process of exchange. A Common European Framework for the systematic and uniform application of new technologies in the collection, preservation, use and exchange of electronic evidence should be based on clear and specific rules for the collection of electronic evidence, common definitions and standards and approximation of legal procedures. The framework should furthermore be fit-for-purpose to keep up with rapidly developing technologies and to cover the specific nature of electronic evidence collection. Investigative measures can have a high impact on the suspect's fundamental rights, especially in a digital environment, which allows gathering (personal) information through different channels. Consequently, there must be a balance between effective law enforcement on the one hand and proper protection of citizens' fundamental rights on the other hand. While realising the Common European Framework the opportunity should be taken to address specific challenges such as cloud computing, admissibility, data collected by SIS (actionable intelligence), transfer and exchange, data retention and virtual currencies. All the actions proposed in the Roadmap should lead to modernisation and harmonisation of legislation and policy, including international law and treaties and adapting it to new technologies. The challenges identified in this Roadmap cannot be addressed without clear policies reflecting the objectives to enhance legislation, law enforcement, trust and technical standards.

LEAs are left to operate in a field of patchwork solutions and playing catch up and manoeuvering their way through a highly uncertain and politically sensitive landscape filled with legal lacunae. Most of the law enforcement challenges, which are plentiful, would primarily find a solution through legislative and/ or policy action. However, there are several actions that can be taken within the LEA community and the digital forensics community. An enhanced enforcement scheme should include many elements to address the law enforcement challenges, such as access to tools and training, solutions for law enforcement databases and uniform guidelines on handling electronic evidence. Improving law enforcement should furthermore be achieved by professionalisation in the field of digital forensics.

Professionalisation in the sub-discipline of digital forensics is necessary to achieve a certain level of professionalism and recognition within this young field. This requires standardisation efforts, reassessing potential regulation of digital forensics professions to ensure that practitioners meet a certain standard, validation of tool to ensure they are fit-for-purpose and accreditation for digital forensic labs to ensure that they meet certain pre-determined quality levels. Professionalisation in the field of digital forensics will complement law enforcement.

18.6 The EVIDENCE Road Map and the Future of Electronic Evidence in Europe

Table 18.2 shows the relationship between the objectives identified into the EVIDENCE Road map and the existing initiatives touching upon the electronic evidence domain. The matching of the EVIDENCE road map objectives with the goals of other Initiatives at EU level are described.

Because of this description, it is to be pointed out that some initiatives touch directly on the objectives of the EVIDENCE road map. It seems that time is enough mature for facing those issues related to enhancing exchange and legal provisions, as well as for taking care of LEAS operational issues. Also, trust and technical standards are considered by some initiatives. Certainly, these activities involve some future research work to produce further developments and achievements, while the focus on professionalisation in the field of digital forensics is still very low.

The important link of the EVIDENCE Roadmap with other complementary initiatives, such as e-Codex is now well established and formalised considering that the EVIDENCE2e-Codex Project and the EXEC- Electronic Xchange of e-Evidences with e-CODEX project, are now financed by EC (e-Justice Programme calls) and will kick off their activities in 2018. These two new initiatives will aim at bringing together and put into practise the EVIDENCE results and achievements as stated into the Road map by means of the e-Codex secured and trusted infrastructure to allow the implementation of the EIO and the exchange of evidence among different Member States.

A part from the various projects running in the EU contexts it is to be noted that the EVIDENCE Road Map is now formally linked also to the institutional activities carried out on electronic evidence by the European Commission and the Council.

The most important ones are the e-Evidence Project on the realisation of an online platform for the Exchange of EIO requests and evidence (e-Justice DG)[21] and

[21] See chapter *Present and future of the exchange of electronic evidence in Europe* by M. A. Biasiotti.

Table 18.2 Relationship between the objectives identified into the EVIDENCE Road map and the existing initiatives related to the electronic evidence domain

Project/initiative	Coordinated by	Topic	EVIDENCE RoadMap objectives
EVIDENCE	CNR-ITTIG, Institute of Legal Information Theory and Techniques of the National Research Council of Italy	Electronic evidence handling and exchange cross-border cooperation	All objectives
e-EVIDENCE	European Commission Directorate-General for Justice and Consumers	European Investigation Order (EIO), Electronic evidence exchange, Reference Implementation Portal	– Objective 2: Further research; – Objective 3: Enhanced legal provisions; – Objective 4: Enhanced exchange; – Objective 5: Enhanced trust; – Objective 6: Enhanced technical standards; – Objective 7: Enhanced legal framework; – Objective 8: Enhanced policies
EVIDENCE2e-CODEX	CNR-ITTIG, Institute of Legal Information Theory and Technicques of the National research Council of Italy	Electronic evidence exchange, EIO and MLA e-Codex Infrastructure	– Objective 1: Enhanced law enforcement; – Objective 2: Further research; – Objective 3: Enhanced legal provisions; – Objective 4: Enhanced exchange; – Objective 5: Enhanced trust; – Objective 6: Enhanced technical standards; – Objective 7: Enhanced legal framework; – Objective 8: Enhanced policies; – Objective 9: Enhanced law enforcement

(continued)

Table 18.2 (continued)

Project/initiative	Coordinated by	Topic	EVIDENCE RoadMap objectives
EXEC	Ministry of Justice of Austria	Exchange European Investigation Orders (EIO) and related e-Evidences fully electronically	– Objective 3: Enhanced legal provisions; – Objective 4: Enhanced exchange; – Objective 5: Enhanced trust; – Objective 6: Enhanced technical standards; – Objective 7: Enhanced legal framework; – Objective 8: Enhanced policies
me-CODEX	Ministry of Justice of North Rhine-Westphalia, Germany	Maintenance of the infrastructure realized by the e-Codex Project	– Objective 4: Enhanced exchange; – Objective 5: Enhanced trust
e-CODEX	Ministry of Justice of North Rhine-Westphalia, Germany	Cross-border e-Justice in Europe	– Objective 4: Enhanced exchange; – Objective 5: Enhanced trust
e-MLA	INTERPOL	Mutual Legal Assistance Requests Forms	– Objective 1: Enhanced law enforcement; – Objective 3: Enhanced legal provisions
MLA Tool	UNODOC	Mutual Legal Assistance Requests Forms drafting	– Objective 1: Enhanced law enforcement; – Objective 3: Enhanced legal provisions
Cybercrime Programme	Council of Europe	International Cooperation, Cybercrime, Electronic evidence treatment and exchange	– Objective 1: Enhanced law enforcement; – Objective 2: Further research; – Objective 3: Enhanced legal provisions; – Objective 4: Enhanced exchange; – Objective 7: Enhanced legal framework; – Objective 8: Enhanced policies

(continued)

Table 18.2 (continued)

Project/initiative	Coordinated by	Topic	EVIDENCE RoadMap objectives
ASGARD-ANALYSIS SYSTEM FOR GATHERED RAW DATA	Vicomtech-IK4 Visual Interaction and Communication Technologies	Tool set for the extraction, fusion, exchange and analysis of Big Data including cyber-offenses data for forensic investigation	– Objective 1: Enhanced law enforcement; – Objective 2: Further research; – Objective 4: Enhanced exchange; – Objective 6: Enhanced technical standards; – Objective 7: Enhanced legal framework; – Objective 9: Enhanced law enforcement; – Objective 10: Professionalisation in the field of digital forensics.
e-CRIME	TRILATERAL RESEARCH & CONSULTING LLP	Economic impacts of cyber crime	– Objective 1: Enhanced law enforcement; – Objective 2: Further research; – Objective 3: Enhanced legal provisions; – Objective 8: Enhanced policies
GIFT	Netherlands Forensic Institute	Forensic toolbox for CBRN incidents	– Objective 1: Enhanced law enforcement; – Objective 2: Further research; – Objective 10: Professionalisation in the field of digital forensics; – Objective 6: Enhanced technical standards
e-SENS	Ministry of Justice of North Rhine-Westphalia, Germany	Cross-border Public services, EU digital single market	– Objective 2: Further research; – Objective 3: Enhanced legal provisions; – Objective 4: Enhanced exchange; – Objective 5: Enhanced trust

(continued)

Table 18.2 (continued)

Project/initiative	Coordinated by	Topic	EVIDENCE RoadMap objectives
LASIE	Engineering – Ingegneria Informatica Spa	Forensic tools, data extraction, electronic evidence	– Objective 1: Enhanced law enforcement; – Objective 2: Further research; – Objective 3: Enhanced legal provisions; – Objective 4: Enhanced exchange; – Objective 10: Professionalisation in the field of digital forensics.
SIIP- Speaker Identification Integrated Project	VERINT	Suspect identification solution based on a novel Speaker Identification (SID) engine and Global Info Sharing Mechanism (GISM)	– Objective 1: Enhanced law enforcement; – Objective 2: Further research; – Objective 6: Enhanced technical standards; – Objective 8: Enhanced policies

the *Inception act Assessment*, for a legislative proposal on *Improving cross-border access to electronic evidence in criminal matters*.[22]

The latter initiative aims to address obstacles in cross-border access to electronic evidence in criminal investigations. Access should become more efficient and faster, while ensuring at the same time transparency and accountability, a high level of protection of fundamental rights including individuals' rights in criminal proceedings, data protection and privacy. It aims at the same time to ensure legal certainty by eliminating or at least reducing fragmentation and conflicts of law. It would also provide an alternative to data localisation requirements that could be imposed by Member States if data in other Member States is too difficult to access.

The impact assessment will develop various policy options based on further analysis, focusing particularly on the following possible measures at EU level.

1. A legal framework authorising authorities to directly request or compel a service provider in another Member State to disclose e-evidence processed in the Union, including appropriate safeguards and conditions. This framework can leave to the discretion of the service provider a decision on whether to provide a response ("production request") or can obligate service providers to respond ("production order"). This could also be considered with respect to service providers located

[22]Inception Impact Assessment (Ares(2017)3896097), available at https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3896097_en.

outside of the Union and/or data stored outside of the Union. This system could be complemented by an obligation for service providers established in third countries but offering services in the EU to designate a legal representative in the EU for cooperation based on production requests/orders.
2. A legal framework for law enforcement to access e-evidence pursuant to a set of safeguards and measures to mitigate cross-border effects, without cooperation of a service provider or the owner of the data, through a seized device or an information system. This could also be considered with respect to data whose storage place is not known or data that is stored outside of the Union.
3. A legal framework to provide for a common understanding of types of electronic evidence and service providers that fall within the scope of the measures proposed.
4. Initiating negotiations with key partner countries such as the U.S. to enable reciprocal cross-border access to electronic evidence, particularly on content data, and including appropriate safeguards.
5. Assessing the role of the EU towards the Council of Europe Budapest Convention on Cybercrime, in view of the negotiations on a second Additional Protocol to the Convention.

The above cited points of the Inception Impact Assessment are objectives that are common to what is stated into the EVIDENCE Road map.

Furthermore, in the Data collection paragraph of the *Inception Impact Assessment* the reference and link to the EVIDENCE project achievements and results is clearly stated whereas the document says "*…The Commission has conducted an expert consultation starting in July 2016 and issued in September 2016 a questionnaire to Member States. …Furthermore, many studies have been conducted on the problem of access to evidence across borders, including the recently concluded and EU-funded EVIDENCE project, which provides further data for the impact assessment*."

So, the EVIDENCE Project Roadmap is now formally linked to the European Commission Strategy on Security and in the EC initiatives on the electronic evidence domain and cross border access to electronic evidence. It is necessary now to concretely put in practise the exchange of electronic evidence in EU by putting together all the initiatives that are going on and aligning them to the unique and common final goal.

Reference

Aulitano S (2016) E-evidence in the European Union. In: De Zan T, Aulitano S (eds) EUnited Against Crime: Improving Criminal Justice in European Union Cyberspace, IAI Documents, 16–17 November 2016