National Disclosure Improvement Plan

Progress update

NPCC National Police Chiefs' Council

College of Policing

CPS

National Disclosure Improvement Plan Phase Two – Embedding Culture Change and Continuous Improvement

This has been an exceptionally busy period for work under the National Disclosure Improvement Plan. This report sets out the progress we have made over the course of the last 12 months and the evaluation of the impact our interventions are having. It demonstrates how we have brought together criminal justice partners at a local and national level to improve our collective confidence, performance and develop our capabilities. Our work has supported the drafting of the revised Attorney General's Guidelines on Disclosure, on which there is to be a public consultation later this year and we have worked with the Transforming Summary Justice Working Groups on changes to the Streamlined Disclosure Certificate which will also be the subject of consultation. The CPS has upgraded its case management system to assist prosecutors with recording decisions taken on disclosure and activities to identify how technology can be used to drive improvements in investigations have continued at pace, coordinated by the cross-agency working group. We have focussed on developing both national and local approaches on issues such as handling sensitive material and extending the use of the Disclosure Management Document.

The College, CPS and the NPCC have also faced a significant challenge on the use of the digital processing notice, which was endorsed by the National Police Chiefs' Council as a way of bringing consistency to the approach to examining digital devices that belong to complainants and witnesses. The expansion of digital and mobile connectivity means that very often there will be evidence that is needed to support the prosecution held on a device belonging to the complainant. Equally, there may be circumstances in which it is necessary to examine particular parts of a complainant's telephone because a fair trial may not be possible if this is not done. We have emphasised in guidance to police and prosecutors that this must not ever be undertaken as a matter of course in all cases, must not be speculative and must be confined to pursuing reasonable lines of enquiry. The digital processing notices are intended to make it clear to complainants how their data may be used, who may see it and why. Investigations and trials must be consistent with protecting the rights of all of those involved, including the privacy rights of complainants and witnesses.

We are awaiting the report of the Information Commissioner into the appropriate legal basis for processing this data and we will review our approach in the light of any recommendations she makes. We expect the report to be published early in the New Year.

We are confident that the management of unused material both as part of the investigation and at the post charge stage across all crime types is in a far better place at the beginning of this year than it was at the beginning of 2018. The data we are now collecting on our performance also makes clear that our task is far from complete. Tackling these issues and improving our resilience in dealing with new technological challenges requires a sustained and long term national response. We cannot do this alone. We need to work even more closely together as investigators and prosecutors and with our criminal justice partners, including the defence. These progress reports are a crucial part of this ongoing effort as we work to ensure the commitments to improve disclosure at every level remain strong.

Key activity

A full list of all of the actions under the NDIP Phase 2 are set out below at Annex A but progress against key measures and initiatives are as follows:

Action: Learning from the on-going pilots led by our cross-agency technology working group will be coupled with evidence from a more detailed wider landscape review undertaken by the NPCC Digital Policing Portfolio. As per the Justice Select Committee recommendation, this work will inform the Home Office, in consultation with the CPS, the National Police Chiefs' Council and the College of Policing, in their production of a comprehensive strategy to ensure that all 43 police forces are equipped to handle the increasing volume and complexity of digital evidence	**On-going**

In June 2019, the Solicitor General and the Minister for Policing jointly hosted a Technology Summit which brought together senior police and prosecutors, representatives from across the criminal justice system, and experts from the technology industry. The summit focused on the handling of digital evidence disclosure in criminal cases and considered how police and prosecutors can be supported to better handle the increasing volumes of digital evidence.

The NPCC's Digital Policing Portfolio has published its landscape review (Annex C), assessing the high-level solutions currently available in the technology marketplace. One of the outcomes of this and other inter-related work is investment by the NPCC to address a number of potential gaps – particularly in outlining the requirements for a nationally-scalable solution for the redaction of sensitive material, and in ensuring there is ongoing coordination of e-disclosure activity and investment across the different police forces. Redaction is a critical dependency if we are to implement the rebuttable presumption recommendation from the Attorney General's Review of Disclosure. The NPCC is also working in partnership with TechUK to ensure that systems interoperability is at the forefront of this thinking, and following an industry engagement session last Autumn, in conjunction with the Attorney General's Office, are presenting an Outline Business Case to the Digital Policing Board in January 2020 setting out the technology options for the redaction of documents, still images and video.

The pilot activities coordinated by members of the NDIP working group are continuing to explore the use of a range of technical solutions. These tools provide a variety of capabilities, including advanced analysis and artificial intelligence. The pilots are testing both the application of such technology to the criminal justice environment and also the operational requirements and impacts of its use. Particular progress over the last quarter has been made with the pathfinder project run by the Metropolitan Police, where the live application of this software has received positive feedback from police and prosecutors alike. The pilot use of an AI application is currently being undertaken in Surrey with a report due early in 2020.

The Home Office, Attorney General's Office, Ministry of Justice, CPS, and Policing all continue to collaborate closely in this space. In particular, joint work has ensured that a consolidated cross-government view of the requirements to support disclosure will be presented into the next reviews of departmental spending.

Action: Focussing on disclosure in the magistrates' and youth courts. **On-going**

We have identified the key barriers to delivering effective case progression as including the quality of evidence and police files which results in more cases being screened out or being sent back for further investigation by the CPS, and the increase in time taken to work through the process leads to higher attrition rates for both victims and witnesses. As we develop an action plan to tackle the issues we will be focussing on;

- Police and CPS file quality: How can we adopt best practices on case file preparation from police forces to increase the rate of the National File Standard being met?
- Engagement with Victims and Witnesses: How can we improve our processes when engaging with victims and witnesses to ensure they stay involved throughout the course of a case?

The National Criminal Justice Board has commissioned a sub-group to examine case progression, led by the Ministry of Justice and the Home Office has also set up a 'task and finish' group to look at case file quality and police and CPS engagement. This group will sit under the sub-group, helping to ensure work is joined up. We welcome both of these work streams as we look to publish a commitment on case progression in the next quarter.

We have also been working on the Streamlined Disclosure Certificate (SDC), with police and prosecutor workshops identifying that having two versions of the SDC, one for cases in which there is material to disclose and one where there is not, is confusing for practitioners. We have therefore proposed a single combined version of the SDC, which will be consulted upon as part of the amendments to the CPIA Code of Practice under the Attorney General's Disclosure Review. Whilst we do not want to detract from the "thinking approach", in which decisions about disclosure are carefully considered and not dealt with as a matter of routine, we are also keen to ensure that what is required is clearly signposted for front-line investigators who may complete SDCs only as an infrequent part of their busy duties.

Action: Continue working with HMCTS to develop a section in the Crown Court Digital Case System accommodating the transfer of unused material and a record of disclosure decisions	**On-going**

A revised Plea and Trial Preparation Form was authorised by the Lord Chief Justice to replace the original PTPH form for new cases, commencing on 22 July 2019. An additional question has been added to the Prosecution Information for PTPH: 'Has a Disclosure Management Document been provided?' The form also makes provision for the defence to indicate whether a served DMD is adequate and if not why not, and also to identify reasonable lines of enquiry and what they say is the appropriate "level of extraction" from mobile devices and computers. The court is required to consider whether they should order a Disclosure Management Document (or an updated one). These amendments should ensure that DMDs are fully utilised from the outset of the case.

Her Majesty's Court and Tribunal Service and the CPS are continuing to work on a section on the Digital Case System accessible by the parties in which disclosed material can be served, together with the MG6C. It is anticipated that this will be available for use in Spring 2020.

Action: Assessing the training needs of prosecutors – ensuring new starters have the opportunity to undertake disclosure training as part of their induction and that recruits receive training appropriate to their level of experience. Evaluate the training provided to prosecutors and plan accordingly for future training based on organisational assessment of user needs.	**On-going**

As part of the Lawyer Induction Programme all new Area prosecutors joining the Crown Prosecution Service receive extended face to face disclosure training over a number of days. In relation to established lawyers, in order to supplement the 2018 proactive disclosure course delivered as part of NDIP phase 1, all lawyers have received a half day training course on the new Code for Crown Prosecutors which is being delivered by Chief Crown Prosecutors and Deputy Chief Crown Prosecutors. This has a particular focus on advising on reasonable lines of enquiry and whether there is any material which might affect the sufficiency of evidence in relation to the Full Code Test.

The following training courses have also been developed and delivered:

- Think Digital Toolkit Videos – data extraction from telephones;
- Use of Disclosure Management Documents in Rape and Serious Sexual Abuse cases.

All prosecutors working in Rape and Serious Sexual Offences Units have received training on the use of Disclosure Management Documents.

The current figures for completion of the College of Policing training on disclosure record that more than a hundred thousand police personnel from Home Office forces have completed all modules of the training, with many more having completed one or more of the six modules.

A disclosure event for Assistant Chief Constables was held, which was well attended. Inputs were designed to update these force strategic leads and CPD was provided via sessions on disclosure handling from both Prosecution and Defence representatives. External academics were involved to encourage alternative approaches and dynamic thinking in relation to approaching cultural reform.

Action: Rolling out the use of DMDs across Crown Court cases and in magistrates' and youth court cases in which there are significant volumes of digital material, communications evidence or third party material	**On-going**

The Disclosure Management Document sets out the approach the prosecution team has taken to disclosure. It should clearly identify what has been considered to be a reasonable line of enquiry in the case and why, together with an explanation of how all seized electronic material has been dealt with. Transparency of the approach is crucial. It should be used to explain to the defence and the court what enquiries are being pursued, and crucially the enquiries we do not intend to make, and why. The DMD should be reviewed regularly. It must be continually updated throughout the life of the case, to form a record of key prosecution strategy, decision making and an audit trail.

The use of the MG3 insert setting out the reasonable lines of enquiry and approach to digital and third party material, together with the DMD has been mandatory in cases dealt with by the Rape and Serious Sexual Offences Units and the Complex Casework Units in the

CPS since March 2018. The Attorney General's Review of disclosure recommended that these be extended to all Crown Court cases by the Summer of 2019. NDIP Phase Two has considered how these might be effectively rolled out.

The NDIP Board initially considered that it would be appropriate to apply some form of criteria to extending the DMD to ensure it is utilised in those cases where it would add value rather than a blanket approach requiring a DMD in all cases. A proposal was discussed with representatives from the judiciary and defence community at the Disclosure Seminar in June 2019 suggesting utilising the DMD in cases where one or more of the following factors were present, regardless of whether they were a Crown Court, Youth or magistrates' court case:

- Substantial or complex third party material, including forensics;
- Digital material in which parameters of search, examination or analysis have been set (likely to include voluminous CCTV, ANPR data as well as digital devices);
- Complex international enquiries which are likely to have a bearing on the case;
- Linked operations;
- Historical offences, especially where there has been a previous investigation.

However, the views from the seminar were that a DMD is capable of adding value in all Crown Court cases, and if the case is very straightforward, then the DMD can also be relatively brief. We are therefore currently piloting the use of the DMD in all Crown Court cases in the CPS Area of Mersey Cheshire. The pilot began in October 2019 and will be for a period of 6 months. We will evaluate the impact of this at the conclusion before making a decision on further extension.

Action: Updating and nationalising police guidelines on data protection and the legal basis for data extraction from digital devices. We will work with victims' groups and relevant Commissioners, including the Investigatory Powers Commissioner, to create clear explanations so that complainants and witnesses understand when, how and why their information will be accessed and processed	**Complete**

The way personal data is used in criminal investigations is an issue of growing significance. Balancing the huge increase in digital information with our duty to respect privacy and ensure all reasonable lines on enquiry are pursued is an important challenge.

The lines of enquiry deemed "reasonable" will depend on the circumstances of each case. This was reinforced by the judgment from the Court of Appeal in R v E [2018] EWCA 2426 (Crim), which confirmed that a fair trial was still possible in a case where a mobile phone had not been seized. In many investigations it will be necessary for the prosecution to look at some personal data but this does not mean access is needed to everything or that it will be automatically disclosed to the defence. There are also important safeguards to prevent complainants being cross-examined on irrelevant sexual history.

The CPS guidance is clear that police and prosecutors must only request data in order to follow a reasonable line of enquiry, which means when it forms an essential part of a fair investigation and prosecution.

We are working with victims' groups to ensure that they understand how, and to what extent, devices will be examined, how data will be used and the circumstances when it will be necessary to share it with the defence. Although much of the publicity surrounding the Digital Processing Notices has been focused on complainants of sexual violence, these are to be used in every case where digital data is a reasonable line of enquiry.

We want every victim to have the confidence to come forward knowing it will be fully investigated and, whenever the evidence supports, charged and fairly prosecuted.

The Information Commissioner will shortly conclude her inquiry into the lawful basis for the processing of the data of victims and witnesses and we will review the consent forms in light of any recommendations from her report.

Action: Reviewing processes for handling sensitive disclosure outside specialist police units and the CPS central casework divisions. This will involve ensuring investigators and prosecutors have the knowledge and skills to deal with cases involving sensitive lines of enquiry and sensitive unused material.	**Complete**

A small working group was set up to review the current processes which are operating in respect of handling sensitive material. It was recognised that different local practices had developed between law enforcement agencies and CPS areas which had the capacity to lead to confusion. Good practice was also identified.

In order to clarify the roles and responsibilities between different law enforcement agencies and prosecutors we have produced a Service Level Agreement (SLA) which articulates the way in which all highly sensitive material ought to be handled and clarifies the roles and responsibilities between the prosecutor and the investigator. These will be implemented in forces and CPS Areas over the course of this year.

We have also produced template documents to be used when making a Public Interest Immunity application to ensure applications are of a consistently high quality and comply with the Criminal Procedure Rules.

The group has reviewed the guidance materials that are available to prosecutors about sensitive material and identified that there was already good legal guidance in place but its positioning meant it was not always easy to locate. These have now all been collated and published on the CPS intranet.

We recognised that there was an absence of clear audit trails about disclosure decisions made for highly sensitive material. The group has produced a Highly Sensitive Disclosure Record sheet (DRS) to serve as a record of the rationale for decisions which are taken throughout the life of a case.

Measuring progress on delivery

The Code for Crown Prosecutors is the authoritative guide to the decision to prosecute. The CPS prosecutes cases when there is sufficient evidence to provide a realistic prospect of conviction, and it is in the public interest to do so. The CPS's role is to prosecute cases firmly, fairly and effectively, paying particular attention to the prosecutor's duties with regard to the disclosure of information to the defence. Careful judgment is required to achieve consistent, high quality decisions throughout the progress of a prosecution.

It is an important part of the duty of the prosecutor to keep every case under continuous review and to bring cases to an end if the Code test is no longer met. On each occasion this occurs, the prosecutor is required to record the reason the case was stopped.

In November 2018 the CPS introduced five new codes for prosecutors to use at the conclusion of every case in which the outcome was not a conviction. In addition, for every case which does not result in conviction, irrespective of the primary reason, the lawyer must record whether issues with disclosure were a contributory factor in the outcome of the case.

These new codes were introduced to improve the data available in order that police and prosecutors can better monitor performance on disclosure, and track the impact of the actions being taken under the National Disclosure Improvement Plan.

The sum of the volumes for primary and secondary reasons do not equal the total number of cases which are recorded as having had disclosure issues. This is as a result of a number of cases being finalised with both a primary and secondary disclosure reason being recorded, so they are counted twice for the purposes of the statistics. Disclosure is an integral part of every case, making it more likely that it will be a feature in cases that do not result in a conviction. The categorisation could mean that disclosure was not timely, or that issues came to light that were not known or could not have been anticipated at the point of charge.

Please note the CPS Caveats relating to the data, full details can be found in Annex B of this document.

Quarter	Cases where disclosure was the primary reason for non-conviction		Cases where disclosure was a contributing factor to the reason for non-conviction	
	Number of cases	% of all cases	Number of cases	% of all cases
18/19-Q3 (Nov-Dec only)	618	6.0%	957	9.3%
18/19-Q4	751	4.8%	959	6.2%
19/20-Q1	592	4.2%	615	4.4%
19/20-Q2	545	3.5%	571	3.7%

This data is to be discussed at a local level by each police force and CPS Area in their joint Prosecution Team Performance Meeting, which are held each month. The data is now broken down by the reason for the disclosure issue, which allows for a close and transparent examination of performance.

Primary Reasons

Quarter	Total primary disclosure reasons	D77 Police / Investigator cause, including the timeliness and quality of disclosure as % of total non-conviction reasons		D78 CPS cause, including timeliness and quality of disclosure as a % of total non-conviction reasons		D79 Other party cause (for example the failure of a third party to provide requested material), including timeliness and quality of disclosure as a % of total non-conviction reasons		D80 No fault: Timeliness and quality acceptable but disclosure was a factor as a % of total non-conviction reasons		D81 No fault: Public interest immunity issues as a % of total non-conviction reasons	
		Volume	%	Volume	%	Volume	%	Volume	%	Volume	%
18/19-Q3 (Nov-Dec only)	**618**	**407**	3.9%	81	0.8%	16	0.2%	104	1.0%	10	0.1%
18/19-Q4	751	469	3.0%	113	0.7%	15	0.1%	132	0.8%	22	0.1%
19/20-Q1	592	376	2.7%	98	0.7%	17	0.1%	81	0.6%	20	0.1%
19/20-Q2	545	419	2.7%	78	0.5%	15	0.1%	18	0.1%	15	0.1%

Secondary reasons

Quarter	Total disclosure focus reasons	D77 Police / Investigator cause, including the timeliness and quality of disclosure as % of total non-conviction reasons		D78 CPS cause, including timeliness and quality of disclosure as a % of total non-conviction reasons		D79 Other party cause, including timeliness and quality of disclosure as a % of total non-conviction reasons		D80 No fault: Timeliness and quality acceptable but disclosure was a factor as a % of total non-conviction reasons		D81 No fault: Public interest immunity issues as a % of total non-conviction reasons	
		Volume	%	Volume	%	Volume	%	Volume	%	Volume	%
18/19-Q3 (Nov-Dec only)	**957**	**340**	3.3%	57	0.6%	95	0.9%	449	4.4%	16	0.2%
18/19-Q4	959	411	2.6%	93	0.6%	90	0.6%	345	2.2%	20	0.1%
19/20-Q1	615	316	2.3%	47	0.3%	63	0.4%	177	1.3%	12	0.1%
19/20-Q2	571	362	2.3%	83	0.5%	42	0.3%	81	0.5%	3	0.0%

As a consequence of collecting more meaningful and granular data, we now have a greater understanding of where issues with disclosure continue to persist. Although there were issues with embedding the use of the new codes, and we are aware of a number of instances in the first quarter of their use where the codes were used incorrectly, the integrity of the data continues to become more reliable as prosecutors become more familiar with when they should be used. Where previously there had been a gap in the provision of clear, comprehensive and trusted information on the handling of unused material by both police and prosecutors, we are now able to target with more precision where further actions are needed.

We continue to see progress and are confident that these numbers will continue to reduce. When mistakes do happen our approach will be positive and supportive so that we can learn from them, work through them as investigators and prosecutors, and use them to improve our performance for the future.

Next steps

We are continually learning lessons and refining our approach, and recognise there is always more to do to improve. Our primary focus is on maintaining momentum to ensure that we maximise the impact of improvement activity across the full breadth of the National Disclosure Improvement Plan. We look forward to the report of HM Crown Prosecution Inspectorate on Crown Court cases and have cautious optimism about the direction of travel. We also anticipate a consultation on amendments to the CPIA Code of Practice and the Attorney General's Guidelines, as well as the report from the Information Commissioner on the appropriate basis for the processing of the data of complainants and witnesses.

There is a strong desire across each of our organisations for continued leadership on disclosure and we recognise that any stepping back from this challenge would jeopardise the progress we have made so far.

M. Cunningham

Max Hill

Nick Ephgrave
National Police Chiefs' Council

Mike Cunningham
College of Policing

Max Hill QC
Crown Prosecution Service

Annex A: Progress against the actions

Item	NDIP actions	Timescale	Status
	CAPACITY		
1	Learning from the on-going pilots led by our cross-agency technology working group will be coupled with evidence from a more detailed wider landscape review undertaken by the NPCC Digital Policing Portfolio. As per the Justice Select Committee recommendation, this work will inform the Home Office, in consultation with the CPS, the National Police Chiefs' Council and the College of Policing, in their production of a comprehensive strategy to ensure that all 43 police forces are equipped to handle the increasing volume and complexity of digital evidence.	On- going	A Tech Summit took place on 10 June 2019. A landscape review identified key national initiatives that included a new Redaction Project Team and a new eDisclosure co-ordination role.
2	Developing processes to ensure that when the investigator seeks a charging decision, whether from a supervising officer or from a prosecutor, information on the lines of enquiry that have been pursued will be supplied as part of the pre-charge file. Ensuring that investigators document what has been considered a reasonable line of enquiry in the circumstances of the case in all requests to prosecutors for charging decisions.	Summer 2019	An evaluation on the effective provision of reasonable lines of enquiry is taking place before these processes are implemented.
3	Continue working with HMCTS on developing a section in the Crown Court Digital Case System accommodating the transfer of unused material and a record of disclosure decisions.	On- going	The creation of new sections on the Digital Case System have been agreed.
4	Evaluating the third party material protocol in 12 months' time and assess whether it is improving the quality of third party disclosure handling.	June 2019	Complete.
5	Rolling out the use of DMDs across Crown Court cases and in magistrates' and Youth court cases in which there are significant volumes of digital material, communications evidence or third party material.	Summer 2019	A 6 month pilot commenced in October, extending the use of the DMD for all Crown Court cases in a CPS Area.
6	Exploring standardisation of terminology in the preparation of disclosure schedules and exploring the recommendation of the Attorney General's Review that a	June 2019	To be taken forward via the Disclosure Manual.

	standard system be developed to provide more information about the nature of material and its potential relevance to the case.		
	CAPABILITY:		
7	Assessing the training needs of prosecutors – ensuring new starters have the opportunity to undertake disclosure training as part of their induction and that recruits receive training appropriate to their level of experience. Evaluate the training provided to prosecutors and plan accordingly for future training based on organisational assessment of user needs.	Spring/Summer 2019	Complete.
8	Continuing the development of the champions' network across policing and CPS, making sure that there is sufficient capacity and capability to drive change. Bringing together police and prosecutor champions with both local events and national conferences to further embed the force champions network and link that into the CPS champions.	June 2019	Both local and national events have taken place across the country, bringing together the champions' network across policing and CPS.
9	Updating and nationalising police guidelines on data protection and the legal basis for data extraction from digital devices. We will work with victims groups and relevant Commissioners, including the Investigatory Powers Commissioner, on informing complainants and witnesses about how their information will be accessed and processed.	Autumn/Winter 2019	See update.
10	Refreshing the Disclosure Manual to reflect new guidance and process under the NDIP.	Spring 2019	Completed. Refreshed disclosure manual was published in December 2018.
11	Developing training and toolkits on digital extraction and tools for analysis for investigators and prosecutors and raising awareness of developments with stakeholders across the criminal justice system.	Spring/Summer 2019	Complete.
12	Reviewing processes for handling sensitive disclosure outside specialist police units and the CPS central casework divisions. This will involve ensuring investigators and prosecutors have the knowledge and skills to deal with cases involving sensitive lines of enquiry and	June 2019	A new SLA has been drafted and new casework products have been developed to assist with audit trails and guidance materials.

	sensitive unused material.		
13	Evaluating the impact of the National Disclosure Standards in the next 12 months to assess whether they have achieved improvements in the service of properly completed and endorsed disclosure schedules.	June 2019	Complete.
14	Considering, in accordance with the timescales contained in NDIP1, whether a licence to practise could assist to drive up police standards in disclosure practice.	January 2019	Complete.
	LEADERSHIP:		
15	Utilising the CPS Disclosure Champions to perform a key role in compliance and assurance at a local level by undertaking local observation to assess change.	Spring 2019	A network of CPS Disclosure Champions is fully established, supporting the delivery of high quality casework by embedding disclosure as a core skill.
16	Encouraging the inclusion of disclosure as part of Continuing Professional Development for police practitioners and driving learning through all levels within forces.	On-going	The College disclosure product allows forces to adopt classroom based or individual training, supporting initial learning and CPD.
17	Raising awareness of disclosure improvement initiatives such as the Disclosure Management Document throughout the criminal justice system.	On-going	Disclosure Forums, both at a national and local level, continue to engage in disclosure improvement initiatives that impact on the Criminal Justice System.
18	Maintaining the leadership momentum in the CPS by repeating the Disclosure Seminar, chaired by the Director of Public Prosecutions on a bi-annual basis.	On-going	Complete. Bi-annual seminars are taking place.
19	Focussing on disclosure in the magistrates' and youth courts.	Autumn/Winter 2019	Work is on-going for a number of initiatives that focus on improving disclosure performance in the magistrates' and youth courts.

20	Making disclosure improvement in the Area a specific objective for Chief Crown Prosecutors against which their performance will be measured.	Spring 2019	Complete. This is a specific performance objective for the most senior leaders in the CPS.
	PARTNERSHIP:		
21	Bringing compliance with disclosure obligations forward, for example in the provision of schedules at the pre-charge stage, has brought significant benefits in some case types. Senior police leaders and prosecutors will work together to identify where this could be achieved in each force.	Autumn/Winter 2019	On-going consultation.
22	Exploring the possibility of bringing a formalised structure to pre-charge engagement between investigators and prosecutors and those representing the suspect, particularly in cases where there is a large volume of digital material that is potentially relevant. The potential to formalise this process is being considered with input from defence stakeholder groups.	October 2019	Draft pre-charge engagement Guidelines, will be published for consultation by the AGO later this year.
23	Replicating the National Disclosure Forum at a local level to facilitate discussions between stakeholders on issues that arise locally.	May 2019	Forums and meetings have taken place across the country at a local level.
24	Working with the judiciary to embed the use of the Disclosure Management Document into the Better Case Management processes, including a section on the Plea and Trial Preparation Form.	On-going	Complete.
25	Building on the experiences of what works well in our most complex casework, a streamlined version of the Early Case Planning Conference will be adopted in all Threshold Test charged cases to facilitate communication between the investigative team and the prosecutor.	Spring 2019	A pilot is being formulated to use ECPCs in all Crown Court Threshold Test cases in a CPS Area.
	GOVERNANCE:		
26	Delivery against the commitments in this plan will continue to be overseen by the National Police Chiefs' Council, the Director of Public Prosecutions and the College of Policing. An update on progress will be published quarterly.	On-going	The Delivery Board meets monthly and quarterly updates on progress are issued.
27	Improving the granularity of data captured in cases which did not result in a conviction but where disclosure was the primary or contributory reason for the	Autumn/Winter 2019	Complete.

	decision to stop the case.		
28	Developing automated data collection in relation to key stages of the disclosure process which will show levels of compliance by both police and CPS such as the identification of reasonable lines of enquiry (pre-charge), creation/management of the Disclosure Management Document/Disclosure Record Sheet and completion of schedules.	Autumn/Winter 2019	CMS underwent a significant development upgrade in June 2019 and a further enhancement will take place in Spring 202.

Annex B: CPS Data Caveats

The disclosure dashboard is for internal management purposes only. It, nor any part of it, should be published without direct permissions from the CPS.

Any publication would breach the UK Statistics Authority Code of Practice (for the release of statistics).

1. CPS data are available through its Case Management System (CMS) and associated Management Information System (MIS). The CPS collects data to assist in the effective management of its prosecution functions. The CPS does not collect data that constitutes official statistics as defined in the Statistics and Registration Service Act 2007.

2. These data have been drawn from the CPS's administrative IT system, which (as with any large scale recording system) is subject to possible errors with data entry and processing. The figures are provisional and subject to change as more information is recorded by the CPS. We are committed to improving the quality of our data and from mid-June 2015 introduced a new data assurance regime which may explain some unexpected variance in some future data sets.

3. The official statistics relating to crime and policing are maintained by the Home Office (HO) and the official statistics relating to sentencing, criminal court proceedings, offenders brought to justice, the courts and the judiciary are maintained by the Ministry of Justice (MOJ).

Defendant 'outcomes' are counted by the CPS at finalisation.

All cases resulting in an outcome other than a conviction are allocated a reason why the case failed. If more than one reason applies the principle reason is chosen.

In pre-charge decision cases all cases resulting in a decision to take no further action for either evidential or public interest reasons are allocated a reason for that decision If more than one reason applies the principle reason in chosen.

Annex C: e-Disclosure Landscape Review, May 2019

Please see below

DIGITAL POLICING PORTFOLIO

e-Disclosure Landscape Review

May 2019

NPCC
National Police Chiefs' Council

Table of Contents

Classification

CLASSIFICATION	
Government Security classification:	Not Protectively Marked
Disclosable under FOIA 2000	Yes

Glossary of acronyms

ABBREVIATION	DEFINITION
AI	Artificial Intelligence
API	Application Programming Interface
BWV	Body Worn Video
APCC	Association of Police and Crime Commissioners
CC	Chief Constable
CCTV	Closed Circuit Television
CI	Chief Inspector
CJ	Criminal Justice
CJS	Criminal Justice System
CJU	Criminal Justice Unit
CoP	College of Policing
CPIA	Criminal Procedure and Investigations Act
CPS	Crown Prosecution Service
DAMS	Digital Asset Management System
DASA	Defence and Security Accelerator
DCF	Digital Case File
DCS	Detective Chief Superintendent
DDI	Data Driven Insights
DEMS	Digital Evidence Management System
DETS	Digital Evidence Transfer Service
DF	Digital First
DII	Digital Intelligence and Investigation
DMD	Disclosure Management Document
DMI	Digital Media Investigator
DPA	Data Protection Act
DPP	Digital Policing Portfolio
DSTL	Defence Science and Technology

ABBREVIATION	DEFINITION
EIA	Early Investigative Advice
ESI	Electronically Stored Information
FOIA	Freedom of Information Act
FTK	Forensic Tool Kit
HMIC	Her Majesty's Inspectorate of Constabulary
HMICFRS	Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services
HMCPSI	Her Majesty's Crown Prosecution Service Inspectorate
HOSB	Home Office Statistical Bulletin
IHM	Information Handling Model
IT	Information Technology
NDAS	National Data Analytics Solution
NDDB	National Disclosure Delivery Board
NDIP	National Disclosure Improvement Plan
MME	Multimedia evidence
NPCC	National Police Chiefs' Council
NTWG	National Technology Working Group
PCC	Police and Crime Commissioners
POLE	People, Objects, Locations and Events
RFI	Request For Information
RIPA	Regulation of Investigatory Powers Act
RLOE	Reasonable Lines of Enquiry
SOC	Scenes of Crime
SME	Subject Matter Expert
TAR	Technology Assisted Review
TWIF	Two-Way Interface
UK	United Kingdom
VRI	Video Recorded Interview

1. Executive Summary

> Disclosure is the process in a criminal case by which someone charged with a crime is provided with copies of, or access to, material from the investigation that is capable of undermining the prosecution case against them and/or assisting their defence. Without this process taking place a trial would not be fair.[1]
>
> **(The Government's Review of the efficiency and effectiveness of disclosure in the criminal justice system)**

The Criminal Procedure and Investigations Act (CPIA) 1996 sets out the broad framework of disclosure obligations on law enforcement and prosecutors to provide the defence with copies of, or access to, any material which might reasonably be considered capable of undermining the case for the prosecution against, or of assisting the case for, the accused. This is with specific reference to unused material that may be relevant to the investigation (i.e. which has been retained but does not form part of the case for the prosecution against the accused).

Prosecutors must provide the defence with the schedules of all of the unused material (disclosure schedules), as well as with copies of any disclosable material. It is the police's responsibility to prepare and provide the prosecutor with disclosure schedules, as well as drawing the attention of the prosecutor to any material an investigator has retained which may satisfy the test for prosecution disclosure. It is the prosecutor's responsibility to ultimately determine whether material is disclosable to the defence.

Definition: Electronic Disclosure (e-Disclosure)

e-Disclosure refers to the disclosure of electronically stored information (ESI). This includes any document/material held in electronic form, including, for example, emails, text messages and voicemail, word-processed documents and databases, and documents stored on portable devices such as memory sticks and mobile phones.

As well as documents that are readily accessible from computer systems and other electronic devices and media, it includes documents that are stored on servers and back-up systems and documents that have been deleted. It also includes metadata and other embedded data.

Key Findings:

The purpose of this review was to: -

- consider the current challenges and review the current e-Disclosure landscape within policing;
- provide an overview of the key capability requirements which may be met by technological solutions; and
- provide an understanding of the possible technological solutions currently available in the marketplace.

The key findings of this e-Disclosure Landscape Review are: -

1.1 Technology is contributing to the challenges of e-Disclosure but can also be an enabler to solve them.

As much as technology creates challenges with the proliferation, in terms of the volume and types of, information, it is also a necessary part of the solution. Traditional methods for cataloguing and finding information are limited. New technologies are capable of vastly

[1] https://www.gov.uk/government/publications/review-of-the-efficiency-andeffectiveness-of-disclosure-inthe-criminal-justice-system

improving the way we search, group and review information and they are the only effective way to manage rapidly expanding data volumes. Technologies to manage data on this scale must be implemented holistically, considering the lifecycle of technology adoption and coupled with processes and policies to manage change and the implementation of new services.

The significant range of law enforcement information infrastructure, in terms of maturity, capacity and inherent information management functionality, does not lend itself to a 'one solution fits all' approach. In some cases, the 'information housekeeping' required to gain the most from advanced technical techniques and tools for e-Disclosure can easily outweigh the potential gains.

Although it was not possible to provide a complete analysis of e-Disclosure technology through this light touch landscape review, it is clear that a single ideal tool to support the needs of both the technical and investigative elements of digital investigations does not exist in the current marketplace. However, the tools identified did meet many of the key requirements and and could form a significant part of a combined solution.

Given the range of capabilities required and the cross-cutting nature of disclosure across policing, the most likely solution to the shortfall is the rollout of several technologies, some currently in use and some new, linked together where possible with common Application Programming Interfaces (APIs), with a common user interface. This would enable a modular approach to the provision of capability with a full range of advanced features, including audit regime, data analytics and search technology. It would also allow for the agile replacement of outdated technologies, and provide the ability to keep up with technological advances, as appropriate.

1.2 e-Disclosure is a high-profile symptom of a wider digital information management problem that is magnified as the volume of digital information continues to increase.

Successful e-Disclosure hinges upon the core capabilities to efficiently, effectively and accurately:

- Collect **relevant** information from a wide range of digital devices;
- Store the information in a secure way that enables accurate searching, review and analysis;
- Determine relevance where this is not immediately clear;
- Audit disclosure decisions;
- Control sharing of disclosable information.

The review found a **range of shortfalls** in current capability, the main points of which are:

a) At the point of collecting electronically stored information, **differing data formats and accuracy of collection processes** (i.e. failure to retrieve relevant information) provides immediate weaknesses in the e-Disclosure process;

b) There is **no standard** for compatible data storage infrastructure and consistent data indexing and cataloguing to enable accurate retrieval of all Electrically Stored Information (ESI);

c) In relation to data acquisition, there are a number of tools that are adequate, but the **diverse number of tools** highlights the lack of a national solution and consistency of approach;

d) Capability to undertake data search/ discovery across some information and media types is lacking. Various software programmes are in use but **not consistently**, however concerns over accuracy often exist;

e) There is **no comprehensive solution** to give full confidence in the ability to conduct analysis to a common standard across policing;

f) Audit is a key aspect of the review component. **Effective and efficient capture of an audit trail is lacking**. Systems are incompatible at the information level making it very difficult to maintain an audit trail throughout the e-Disclosure process; and

g) There is little support to the disclosure schedule production process which is **time consuming** and an area where it is easy to introduce additional **errors or omissions** to the e-Disclosure process.

1.3 Spiralling volumes of digital information challenges law enforcement to maintain information management strategies and the process of identifying and producing electronic information for disclosure purposes.

The identified challenges relating to e-Disclosure are not unique to policing in England and Wales and are being experienced by law enforcement and private industry worldwide.

Efficient, accurate and timely e-Disclosure is not an add-on function but starts when information is collected and stored. The ability to disclose ESI must not be an afterthought but a continuous aspect throughout the information lifecycle. Therefore, in defining the requirements for e-Disclosure it is necessary to examine the full scope of capability that spans the data capture, storage, acquisition and search components that are usually under the management of the information infrastructure and the analyse, review, produce and release components that are often associated with technology assisted review (TAR). To complicate matters there is no clear boundary between these different information management regimes.

While technology alone will not deliver the full capability, it has the potential to make a significant contribution, but that contribution will not be realised without the corresponding people and process elements.

1.4 Technology to address the problem will help, but it is likely that there will always be a gap.

Despite the work undertaken by national programmes and local force initiatives, there remain several aspects of e-Disclosure where further technology-based intervention is required. Technical solutions by their very nature have embedded processes within them and assume a level of skill and knowledge of the user. Any technology solution must be evaluated not only on the functionality itself, but the compliance of the embedded processes and the training of the user to utilise the technology in the way it was designed.

All these factors must be underpinned by a strong legal and ethical foundation. Questions that already exist in relation to e-Disclosure include how data will be collected and processed, concerns about algorithmic bias & false positives and where the acceptable limits lie in this space.

Key areas for further investment to address the remaining shortfalls include:

Artificial Intelligence (AI): This is a broad term that encompasses a number of related fields, including machine learning (the ability to predict most likely events to occur) or predictive coding (use of a computer system to help determine which documents are representative of a defined category) and deep learning (pushing the boundaries of understanding what is possible), all of which are used in situations where the task is complex or varied. However, the test applied for disclosure is a particularly difficult one for AI to apply. It is also incredibly difficult to identify the factors used to reach its conclusion.

Advanced Search: There are a number of search techniques that require less specific inputs ranging from the use of search operators such as wild cards or exact phrases to the use of word clouds to highlight most regularly used words or phrases. Full text search, which requires a text indexing engine, enables searching all text inside any text-based file. There are also advances in video and image search technologies that would increase the efficiency of finding all relevant data.

Alerts: Alerts or notifications are machine-to-person communications of important and / or time sensitive information. The use of alerts and notifications to notify the user when new information or data is available against saved searches has particular relevance to e-Disclosure.

1.5 Hypothesis

Given the range of capabilities required and the cross-cutting nature of disclosure across policing, the most likely solution to the shortfalls is the rollout of a number of technologies, some currently in use and some new, with common APIs, linked together where possible with a common user interface. This would enable a modular approach to the provision of capability with a full range of advanced features, including audit regime, data analytics and search technology. It would also allow for the agile replacement of out dated technologies, and provide the ability to keep up with technological advances, as appropriate.

Whilst being cognisant of the necessary differences between forces and in priorities,

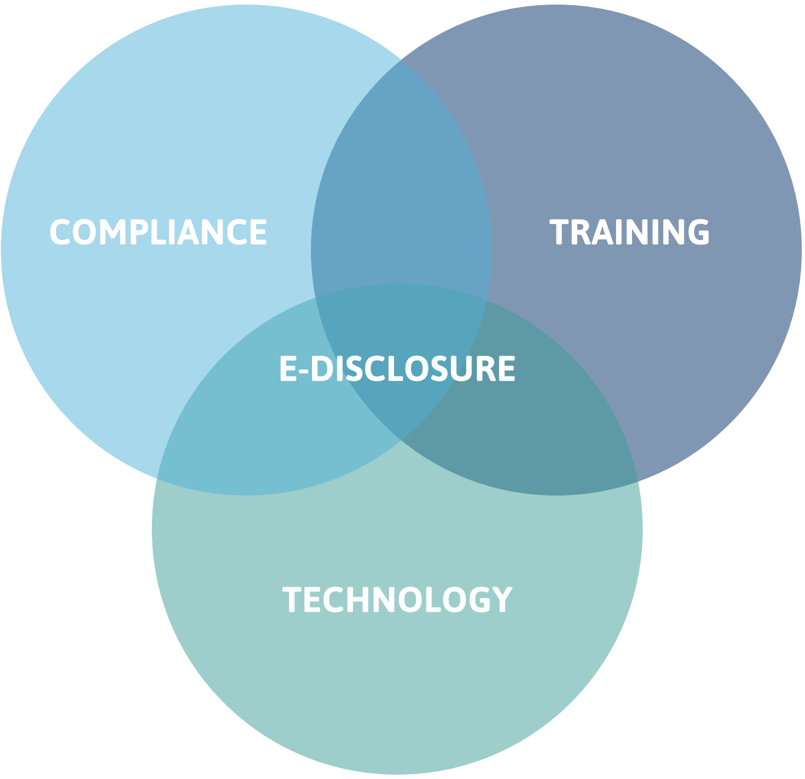
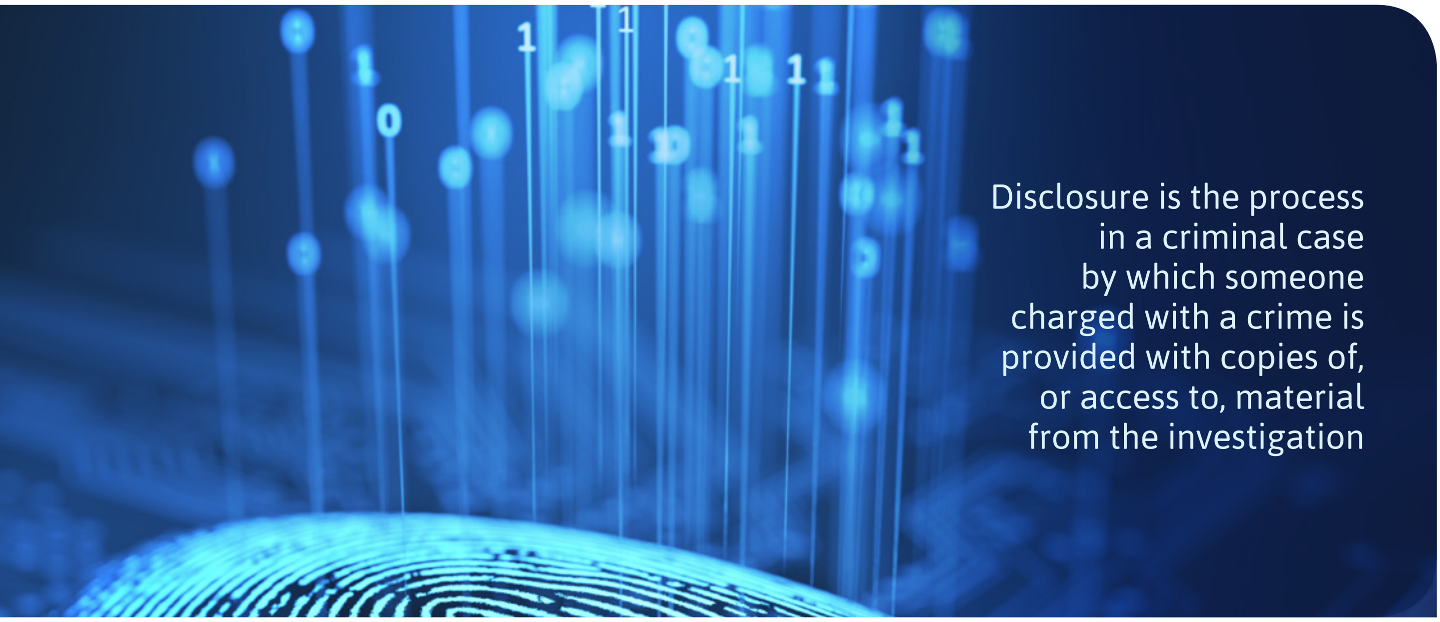


Figure 1 Technology solutions for e-Disclosure are dependent on compliance and training.



Disclosure is the process in a criminal case by which someone charged with a crime is provided with copies of, or access to, material from the investigation

this rollout should be as wide as possible, and scalable, to encourage consistency in both process and technology across policing to enable better coordination.

The most important parts of the solution are likely to be the supporting technology: the common or compatible storage, standards, indexing and cataloguing. Without these the key capabilities of review, search and analysis (which also apply across the rest of the investigation process) cannot be efficient or effective, particularly between forces.

Next Steps: Based on the business challenges and statements of need highlighted in this review, as well as the identified gaps and associated recommendations, the suggested next step would be to assess the above hypothesis as part of an e-Disclosure Outline Business Case that will:

- Conduct more in-depth reviews with representative police forces, including:
  - Capturing the 'as is' process
  - Supporting technologies already in use, and
  - Assessing any other related funded initiatives;
- Engage with the related policing or government initiatives, pilots, proof of concepts to ascertain whether they are addressing any e-Disclosure requirements pertinent to their scope to de-duplicate effort, identify any gaps and maximise any opportunities for collaborative working.
- Identify and assess potential options to deliver against the e-Disclosure requirements that have no other identified delivery mechanism.
- Following the completion of existing proof of concepts/pilots, to select a preferred solution(s) and identify a funding source(s) to support the delivery of an e-Disclosure solution(s) that addresses the key business needs and capability gaps whilst delivering the required business outcomes and benefits.

2. Introduction

The Criminal Procedure and Investigations Act (CPIA) 1996 sets out the broad framework of disclosure obligations on law enforcement and prosecutors to provide the defence with copies of, or access to, any material which might reasonably be considered capable of undermining the case for the prosecution against, or of assisting the case for, the accused. This is with specific reference to unused material that may be relevant to the investigation (i.e. which has been retained but does not form part of the case for the prosecution against the accused).

Prosecutors must provide the defence with the schedules of all of the unused material (disclosure schedules), as well as with copies of any disclosable material. It is the police's responsibility to prepare and provide the prosecutor with disclosure schedules, as well as drawing the attention of the prosecutor to any material an investigator has retained which may satisfy the test for prosecution disclosure. It is the prosecutor's responsibility to ultimately determine whether material is disclosable to the defence.

Ensuring disclosure is right is a fundamental part of a fair criminal justice system. Trials have collapsed or cases have had to be discontinued specifically due to the prosecution having failed to disclose, in a timely manner, vital information pertinent to the case. These failures have led to there no longer being a realistic prospect of conviction, a fundamental consideration as to whether a suspect should be, or continues to be, prosecuted, as outlined in the Code for Crown Prosecutors. In addition to the impact on victims of crime there are wider consequences of disclosure failings including:

- Risk of miscarriages of justice
- Reduced public confidence in policing and the Criminal Justice System
- Significant waste of time, resource and money across all involved in the justice process

> "The disclosure to the defence of material obtained during a criminal investigation, that the prosecution has not used as part of its case is fundamentally important to ensuring a fair trial. Yet, I suspect that no one who has regular professional involvement with the criminal courts can have avoided the conclusion, often from painful experience, that for too long the system of disclosure has not operated effectively enough."[2]
>
> **(The Attorney General, Geoffrey Cox QC MP)**

Several failings in the disclosure process have resulted in the collapse of trials and the successful appeal against unsafe convictions. These failings have resulted in several reviews of disclosure procedures and practice that highlight the need to improve the disclosure process and make a number of recommendations, which in turn has generated a series of key recommendations for change. These reviews include:

- Making it Fair – A Joint Inspection of the Disclosure of Unused Material in Volume Crown Court Cases, July 2017 (HMCPSI, HMIC);[3]
- Mouncher Investigation Report, July 2017;[4]
- Justice Select Committee inquiry, July 2018;[5]
- Attorney General review: "Review of the efficiency and effectiveness of disclosure in the criminal justice system", Nov 2018.[6]

Coordination of these key recommendations for change is delivered through the National Disclosure Delivery Board (NDDB), via the National Disclosure Improvement Plan (NDIP), with ownership being shared between the National Police Chiefs' Council (NPCC), the Crown Prosecution Service (CPS) and the

[2] https://www.gov.uk/government/publications/review-of-the-efficiency-and-effectiveness-of-disclosure-in-the-criminal-justice-system

[3] https://www.justiceinspectorates.gov.uk/cjji/inspections/making-it-fair-the-Disclosure-of-unused-material-in-volume-crown-court-cases/

[4] https://www.gov.uk/government/publications/mouncher-investigation-report

[5] https://www.parliament.uk/business/committees/committees-a-z/commons-select/justice-committee/inquiries/parliament-2017/disclosure-criminal-cases-17-19/publications/

[6] https://www.gov.uk/government/publications/review-of-the-efficiency-and-effectiveness-of-disclosure-in-the-criminal-justice-system

College of Policing (CoP). In its broadest terms, the NDIP sets out:

- What has been done to date about this issue,
- What further work is required against the recommendations, and
- Looks to identify and prepare for anticipated future challenges.

To this end, the NDIP is coordinating activities, under the following strategic priority areas:

- Strengthening the **capacity** to deal with disclosure, ensuring we are fit to meet the challenges we face, both now and in the future;
- Improving the **capability** of police and prosecutors and equipping them with the right skills, particularly in the context of handling large volumes of digital material;
- **Leading** the transformation of the culture of the investigative mind-set, so that disclosure is viewed as an integral part of the investigation and any subsequent prosecution;
- Engaging more effectively in our **partnerships** in the criminal justice system and improving communication between the prosecution and defence at the outset of criminal proceedings; and
- Embedding the actions taken at a national level into local police forces and CPS areas by robust **governance** on both national and local improvement plans.

The **capacity** priority includes recognition of the particular challenges of **e-Disclosure**, which is the disclosure of Electronically Stored Information (ESI). These challenges are reflective of the now ubiquitous nature of digital technology resulting in a rapidly increasing volume, diversity and complexity of potentially relevant ESI.

The Attorney General's Review and the Justice Select Committee inquiry identified the unprecedented challenge that this presents to investigators and prosecutors, citing an example that the average mobile phone today is capable of holding the data equivalent of about 5 million A4 pages;

> "It is clear that the right thing to do in these cases is to adopt new, technology-based approaches to managing this scale of material because its growth is outpacing human capacity to handle it."[7]

Several national programmes and organisations are working closely with the criminal justice community and focusing on the technology element of the NDIP e.g. Digital First (DF), Digital Intelligence & investigation (DII), Transforming Forensics (Digital Forensics), Defence Science and Technology (DSTL).

This Landscape Review was commissioned by NPCC's Criminal Justice lead (AC Nick Ephgrave) to examine and report on the challenges of **e-Disclosure**. The volume of cases that may require e-Disclosure is also increasing precipitously, as stated by the Parliamentary Office of Science and Technology:

> 'The ubiquity of digital devices means that digital evidence may be present in almost every crime.'[8]

[7] https://www.gov.uk/government/publications/review-of-the-efficiency-and-effectiveness-of-disclosure-in-the-criminal-justice-system

[8] https://researchbriefings.files.parliament.uk/documents/POST-PN-0520/POST-PN-0520.pdf

3. Purpose & Approach

In response to the recognition of these challenges, this Landscape Review will:

- consider the current challenges and review the current e-Disclosure landscape within policing;
- provide an overview of the key capability requirements which may be met by technological solutions; and
- provide an understanding of the possible technological solutions currently available in the marketplace.

The scope of the review is limited to the technical element of the required capability with the people, process, training and procedures elements addressed under the NDIP. Notwithstanding the limited scope of the review, in considering current capability and shortfalls, it takes note of the user's likely skill base and knowledge and the process and procedures required to ensure a compliant solution.

The approach to developing this Landscape Review included the following activities:

- **Desktop Review:** A review of the latest reports and recommendations for improvements in | the disclosure process has been carried out, with specific attention to the points relating to digital material;
- **Marketplace Review:** A market place engagement exercise was conducted with techUK, which represents over 900 companies in the tech. industry. A review was carried out of the output from both formal 'Requests For Information' (RFI) and a subsequent round-table discussion at techUK (attended by global, national and small medium enterprises) regarding possible technological solutions currently available in the marketplace;
- **User group review:** A review of the output of a user group workshop held at the Major Investigation Digital Insights Conference, chaired and facilitated by the DII team; In addition, the output from a joint workshop organised by the Ditchley Foundation and Defence and Security Accelerator (DASA), regarding disclosure was also incorporated within this review.
- **Interviews:** Interviews were held with police force representative, technology providers and disclosure SMEs.

The information gathered has been analysed and summarised in the following sections:

- **e-Disclosure in Policing:** this section provides an overview of e-Disclosure in policing and develops a set of key capability requirements for consideration in review of the current technology landscape.
- **Current Technology Landscape:** this section provides a high-level overview of technology, particularly supported by the Marketplace Review and Interviews. It considers both those currently in use in policing as well as developing techniques and capabilities and planned delivery, in the context of the key capability requirements and the e-Disclosure process map defined in the previous section.
- **Gap Analysis:** this section highlights the areas in the current e-Disclosure in policing landscape that do not have an existing or planned solution known at the time of writing this review.
- **Recommendations:** this section provides recommendations to address the gaps identified in the previous section.

4. e-Disclosure in Policing

'e-Disclosure' refers to the disclosure of ESI i.e. any document/material held in electronic form, including, for example, emails, text messages and voicemail, word-processed documents and databases, and documents stored on portable devices such as memory sticks and mobile phones.

As well as documents that are readily accessible from computer systems and other electronic devices and media, ESI includes documents that are stored on servers and back-up systems and documents that have been deleted. It also includes metadata and other embedded data. The definition of e-Disclosure in this context thus becomes the process of identifying, collecting, processing, analysing and reviewing ESI for criminal legal proceedings.

In the context of disclosure, material may be deemed relevant to an investigation if it appears to have some bearing on any offence under investigation or any person being investigated. As well as being broad in scope, this definition applies both to items in isolation or when combined with other material. The process of disclosure, and in particular e-Disclosure due to the rapidly increasing volumes of material involved, therefore hinges upon the key capabilities of efficiently, effectively and in compliance with legislative and procedural requirements doing the following:

- Data Review: Review the extracted relevant material from a wide range of digital devices;
- Data Search: Searching and/or sifting available material;
- Data Analysis: Enriching, analysing, connecting or combining material;
- Data Assess: Assessing material, analysis or combinations of material in order to determine relevance;
- Data Record: Documenting disclosure decisions; and
- Data Reveal: Revealing unused material and schedules to the prosecutor.

In turn these capabilities require the correct triaging at ingest, storing, referencing and handling of material or data throughout its retention period, and in this sense, e-Disclosure requirements impact across the entire investigation process. These data lifecycle activities are presented in the following diagram.

DATA CAPTURE INGEST AND STORAGE	DATA CLEANSING	DATA MANAGEMENT AND ACCESSIS	DATA DISCOVERY AND ANALYSIS	DATA RECORDING AND SHARING
Data triage and acquisition	Deduplication	Data indexing and cataloguing	Data enrichment	Recording and sharing of data and / or metadata
Data entry	Data correction	Information handling model (IHM)	Data mapping / transformation	Recording and sharing of data visualisations and / or supporting metadata
Machine generated data	Data formatting	Review, retain and dispose (RRD) model	Data search and / or sift	
	Deletion of uncorrectable or non compliant data		Data analysis and visualisation	

Figure 2 High Level Data Lifecycle Activities

The following two sections describe the capability requirements and process in more detail.

4.1 Key Capability Requirements

Statements of business need were collated and validated by the National Technology Working Group under the National Disclosure Delivery Board. These business need statements have been reviewed and the following 5 have been identified as relevant to the scope of this e-Disclosure landscape review.

1. Development of nationally consistent standards, common tools, infrastructure or techniques to acquire, store and utilise the increasing amounts of digital material being seized/collected in a legal, ethical and efficient way.
2. Data is currently stored in siloed, unconnected systems or on individual drives. Develop a process that reduces data duplication, allows efficient sharing within forces & between forces, and compliance against management standards is achievable and auditable.
3. Establish methods/processes to ensure identification, grouping or restructuring of large volumes of material (such as telephone number, vehicles, and addresses) is effective, efficient and productive.
4. Creation of a coordinated investment approach in advanced data analytics capabilities, especially for mobile phone records to develop nationally consistent applications across investigations.
5. Assisting in developing a formalised structure to pre-charge engagement between investigators and prosecutors and those representing the suspect, particularly in cases where there is a large volume of digital material that is potentially relevant.

These statements can be deconstructed into their constituent parts to identify some of the key capability requirements for e-Disclosure as shown in the table overleaf.

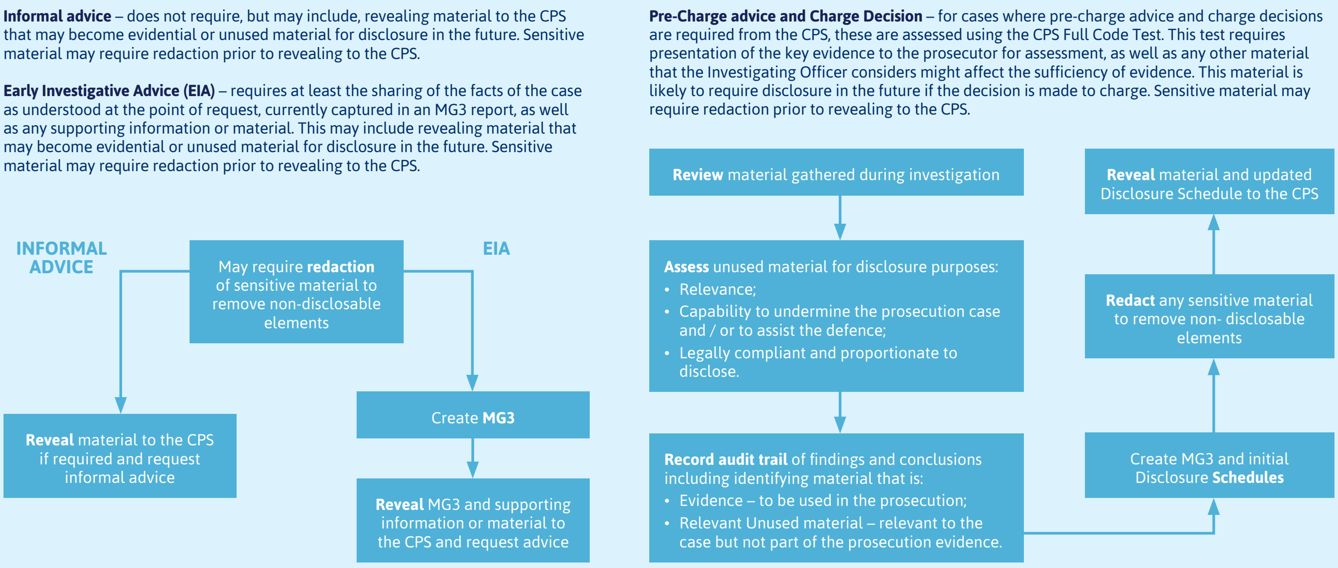
‘e-Disclosure’ refers to the disclosure of Electronically Stored Information i.e. any document/material held in electronic form, including, for example, emails, text messages and voicemail, word-processed documents and databases, and documents stored on portable devices

BUSINESS NEED STATEMENT	KEY CAPABILITY REQUIREMENTS – THERE IS A REQUIREMENT FOR (AN) EFFECTIVE AND EFFICIENT:
1. Development of nationally consistent standards, common tools, infrastructure or techniques to acquire, store and utilise the increasing amounts of digital multimedia material being seized/ collected it in a legal, ethical and efficient way.	• Nationally consistent data standards • Nationally consistent data formats • Nationally consistent data indexing and cataloguing • Nationally consistent or compatible data enrichment capability • Nationally consistent or compatible data acquisition and ingest techniques • Nationally consistent or compatible data storage infrastructure • Nationally consistent or compatible search • Nationally consistent or compatible analytics capabilities • Nationally consistent or compatible summary visualisation capability for digital material • Nationally consistent or compatible data and material sifting and filtering capability
2. Data is currently stored in separate, unconnected systems or on individual drives. Develop a process that reduces data duplication, allows efficient sharing within forces & between forces, and compliance against management standards is achievable and auditable.	• De-duplication across disparate storage • Nationally consistent or compatible data storage infrastructure • Cross force data access capability • Nationally consistent or compatible and auditable data access management • Cross force search capability • Nationally consistent data indexing and cataloguing • Nationally consistent data standards • Nationally consistent data formats • Nationally consistent and auditable data management and standards • Nationally consistent or compatible capability for sharing digital material within and between forces
3. Establish methods/processes to ensure identification, grouping or restructuring of large volumes of material (e.g. telephone number, vehicles, etc…) is effective, efficient and productive.	• Nationally consistent data indexing and cataloguing • Nationally consistent or compatible summary visualisation capability for digital material
4. Creation of a coordinated investment approach in advanced data analytics capabilities, especially for mobile phone records to develop nationally consistent applications across investigations.	• Nationally consistent data analytics capabilities
5. Assisting in developing a formalised structure to pre-charge engagement between investigators and prosecutors and those representing the suspect, particularly in cases where there is a large volume of digital material that is potentially relevant.	• Capability for sharing digital material with prosecution and defence • Capability for sharing analysis of digital material with prosecution and defence

4.2 E-Disclosure Process Map

To aid understanding of the challenges, and to support the identification of where key capability requirements and existing or developing technologies align to the disclosure process, the following high-level business process map diagram has been developed through a review of the latest reports on disclosure procedures and practice.

Pre Charge E-Disclosure Activities – not all activities required for all cases



Informal advice – does not require, but may include, revealing material to the CPS that may become evidential or unused material for disclosure in the future. Sensitive material may require redaction prior to revealing to the CPS.

Early Investigative Advice (EIA) – requires at least the sharing of the facts of the case as understood at the point of request, currently captured in an MG3 report, as well as any supporting information or material. This may include revealing material that may become evidential or unused material for disclosure in the future. Sensitive material may require redaction prior to revealing to the CPS.

INFORMAL ADVICE

May require **redaction** of sensitive material to remove non-disclosable elements

EIA

Reveal material to the CPS if required and request informal advice

Create **MG3**

Reveal MG3 and supporting information or material to the CPS and request advice

Pre-Charge advice and Charge Decision – for cases where pre-charge advice and charge decisions are required from the CPS, these are assessed using the CPS Full Code Test. This test requires presentation of the key evidence to the prosecutor for assessment, as well as any other material that the Investigating Officer considers might affect the sufficiency of evidence. This material is likely to require disclosure in the future if the decision is made to charge. Sensitive material may require redaction prior to revealing to the CPS.

Review material gathered during investigation

Assess unused material for disclosure purposes:

- Relevance;
- Capability to undermine the prosecution case and / or to assist the defence;
- Legally compliant and proportionate to disclose.

Record audit trail of findings and conclusions including identifying material that is:

- Evidence – to be used in the prosecution;
- Relevant Unused material – relevant to the case but not part of the prosecution evidence.

Create MG3 and initial Disclosure **Schedules**

Redact any sensitive material to remove non- disclosable elements

Reveal material and updated Disclosure Schedule to the CPS

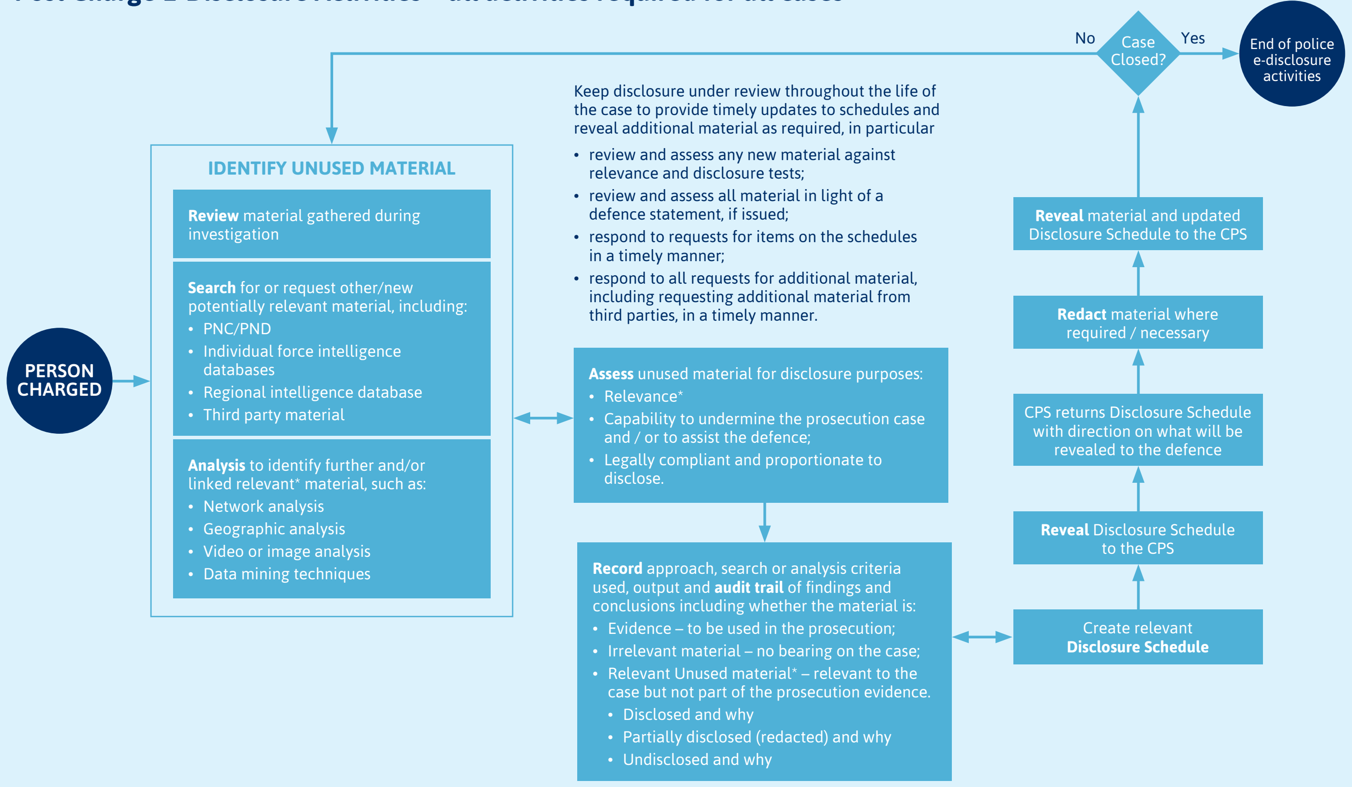
Figure 3 Disclosure process map

The process map was reviewed against the high level scenarios developed as part of the investigation into the context of e-Disclosure. Assessment of the scenarios resulted in the conclusion that the volume, diversity and / or complexity of the ESI would vary, but the high level activities would, on the whole, remain the same, regardless of crime type[9].

The following mapping between the process maps and the key capability requirements further illustrates this as the majority of these key capability requirements are also relevant to activities in the preceding investigation.

[9] Cases which have highly sensitive unused material may involve police supervising the viewing of the sensitive material by the defence

Post Charge E-Disclosure Activities – all activities required for all cases



IDENTIFY UNUSED MATERIAL

Review material gathered during investigation

Search for or request other/new potentially relevant material, including:

- PNC/PND
- Individual force intelligence databases
- Regional intelligence database
- Third party material

Analysis to identify further and/or linked relevant* material, such as:

- Network analysis
- Geographic analysis
- Video or image analysis
- Data mining techniques

Keep disclosure under review throughout the life of the case to provide timely updates to schedules and reveal additional material as required, in particular

- review and assess any new material against relevance and disclosure tests;
- review and assess all material in light of a defence statement, if issued;
- respond to requests for items on the schedules in a timely manner;
- respond to all requests for additional material, including requesting additional material from third parties, in a timely manner.

Assess unused material for disclosure purposes:

- Relevance*
- Capability to undermine the prosecution case and / or to assist the defence;
- Legally compliant and proportionate to disclose.

Record approach, search or analysis criteria used, output and **audit trail** of findings and conclusions including whether the material is:

- Evidence – to be used in the prosecution;
- Irrelevant material – no bearing on the case;
- Relevant Unused material* – relevant to the case but not part of the prosecution evidence.
  - Disclosed and why
  - Partially disclosed (redacted) and why
  - Undisclosed and why

Create relevant **Disclosure Schedule**

Reveal Disclosure Schedule to the CPS

CPS returns Disclosure Schedule with direction on what will be revealed to the defence

Redact material where required / necessary

Reveal material and updated Disclosure Schedule to the CPS

Figure 3 Disclosure process map

KEY CAPABILITY REQUIREMENTS FROM THE BUSINESS PROBLEM STATEMENTS	DISCLOSURE PROCESS MAP ACTIVITIES						
	Review material gathered during investigation	**Search** for other / new potentially relevant material	**Analysis** to identify further and / or linked relevant material	**Record** output, **audit trail** of findings and conclusions	**Assess** unused material for disclosure purposes	**Record** material to be disclosed by creating or updating a Disclosure Schedule	**Share** material and Disclosure Schedule with prosecutor
1. Nationally consistent data standards	X	X	X		X	X	
2. Nationally consistent data formats	X	X	X		X		X
3. Nationally consistent data indexing and cataloguing	X	X	X	X	X	X	
4. Nationally consistent or compatible data enrichment capability	X	X	X		X		
5. Nationally consistent or compatible data acquisition and ingest techniques	X	X	X		X		
6. Nationally consistent or compatible data storage infrastructure	X	X	X		X		X
7. Nationally consistent or compatible search		X					
8. Nationally consistent or compatible analytics capabilities			X				
9. Nationally consistent or compatible summary visualisation capability for digital material	X		X		X		
10. Nationally consistent or compatible data and material sifting and filtering capability	X	X	X		X		
11. Nationally consistent or compatible and auditable data access management	X	X	X	X	X	X	

	DISCLOSURE PROCESS MAP ACTIVITIES						
KEY CAPABILITY REQUIREMENTS FROM THE BUSINESS PROBLEM STATEMENTS	**Review** material gathered during investigation	**Search** for other / new potentially relevant material	**Analysis** to identify further and / or linked relevant material	**Record** output, **audit trail** of findings and conclusions	**Assess** unused material for disclosure purposes	**Record** material to be disclosed by creating or updating a Disclosure Schedule	**Share** material and Disclosure Schedule with prosecutor
12. Nationally consistent and auditable data management and standards	X	X	X	X	X	X	X
13. Nationally consistent or compatible capability for sharing digital material within and between forces	X	X	X		X		
14. Nationally consistent data analytics capabilities			X				
15. Cross force data access capability	X	X	X		X		
16. Cross force search capability		X					
17. De-duplication across disparate storage	X	X	X				
18. Capability for sharing digital material with prosecution and defence				X		X	X
19 Capability for sharing analysis of digital material with prosecution and defence				X		X	X

Through mapping these capabilities and capturing the key characteristics required within the e-Disclosure process the information can be used to assess business needs, technology requirements and align investment with strategic priorities. The following section provides a high-level review of the current technology landscape.

5. Technology Landscape

This section provides an overview of the technology landscape by considering the following:

- current technology used in policing;
- developing techniques and capabilities that could be utilised to assist with disclosure;
- relevant planned delivery.

5.1 Summary of Current Technology in Policing

A number of core technological solutions are already used in policing today which support key aspects of disclosure, however none of the technologies reviewed for this report provide a comprehensive disclosure capability, and they cannot be scaled sufficiently to provide a national platform. They could however provide or inform part of the future solution.

In addition, the improving documentation and auditing of e-Disclosure driven by the introduction and expanding use of the Disclosure Management Document (DMD) encourages consideration of all relevant electronic material but does not in itself improve the capability to review, search for, analyse or assess electronic material for disclosure.

The remainder of this section provides a high-level overview of current technologies used in policing to support disclosure based on the information available in the RFI responses and interviews with technology providers and disclosure SMEs. The specific technologies are not identified to remove any competitive advantage issues.

Review: There are a number of tools identified that appear to provide a good level of capability, providing the material has been imported into an accessible system and is easily found for review, which is currently a significant challenge for many forces. The number of tools does however highlight the lack of a national solution and consistency of approach.

Search: The range of tools identified in this space highlight the lack of consistent, efficient and effective ingest or import of electronic material that is key to the identification of all relevant electronic material for e-Disclosure, as well as the lack of a national solution and consistency of approach. The consistent import or ingest and storage of material is increasingly important to ensure that all relevant material can be found quickly with the rapidly expanding volume of material to be considered. This is relevant not only within a force but across forces as material may have been captured by other forces that is relevant to the case in question.

Analysis: Similar to search, the range of tools identified in this space highlight the lack of consistent, efficient and effective ingest or import of electronic material that is key to the ability to perform effective analysis and identify links or combinations of material relevant for disclosure. It also highlights the lack of a national solution and consistency of approach, and that none of the tools currently in operation appear to provide a sufficiently comprehensive solution to give full confidence in the ability to conduct analysis.

Assess: The technologies identified against this stage in the process are used to view the material or redo or review analysis that supports the relevance of the material for disclosure. The effectiveness of this stage relies heavily on the ability of the Search and Analysis technologies to record, find and analyse the relevant material to enable their assessment.

Record output of review, search and analysis: Although there are capabilities that provide an audit trail of searches and acquisition activities, this review has not identified any technology that particularly supports the effective and efficient capture of an audit trail of findings and conclusions with any supporting reasoning. The conclusions to be made and recorded here require understanding of any handling caveats or sensitivities of the material which should be captured in the indexing or cataloguing of the material, the completeness of the evidential audit trail, as well as the ability to effectively reference or link to the data so that it can be easily found. Clarity of what analysis has and has not been undertaken is critical to successful passage through the criminal justice system, particularly given that understanding of emerging technologies is often limited.

Record (Disclosure Schedule and Disclosure Management Document (DMD)): Technology can support this through the automatic generation of required documentation based on information captured in the previous Record stage. Only one technology has been identified in this review that supports this activity.

Reveal: Technologies that support this activity have been identified in this review that appear to provide a level of capability and are fairly widely used, although not across all forces. However, this process is still partially reliant on manual processes such as scanning in paper documents and producing hard copies of digital images in order to compensate for the lack of a completely intuitive digital capability, resulting in wasted cost on all agencies involved, an increased risk of error and undermines the potential benefits that could be realised from digital working.

Due to its time bound nature it should be noted that this review has not undertaken an in-depth review of all technologies used in the e-Disclosure process, only those referenced in the RFI responses and interviews with technology providers and disclosure SMEs. As such it is recommended that further work is undertaken with policing to identify other relevant technologies currently in use in policing and assess their capability against the requirements.

5.2 Utilisation of technological techniques and capabilities

The case for the utilisation of new technological techniques and capabilities in disclosure has been recognised in a number of court cases, including the 2015 ruling in the UK High Court endorsing the use of Technology Assisted Review (TAR). TAR is a software approach that is increasingly assisting in the identification of relevant material through the use of mathematical algorithms, statistical sampling and machine learning or predictive coding. These court cases are illustrative of the acceptance that although the ***human element cannot be removed*** from the disclosure process, the utilisation of these kinds of technology supported approaches is both necessary and appropriate in order to balance the capacity challenge posed by the increasing volume of material. That said, this has not yet been trialled in the field of criminal justice, which may be naturally less predisposed to the use of such technology. It is clear that, at the very least, being able to provide clarity as to the capabilities applied will be no less important than the capabilities themselves. In addition, the appropriate use and ethical considerations associated must underpin all elements when considering utilising technological techniques and capabilities.

It is important that technology is not considered in isolation. While the required capability will consist of people, process and technology there is a tight relationship between these elements that need to be viewed in a technical context. Technical solutions by their very nature have embedded processes within them and assume a level of skill and knowledge of the user. As depicted in Figure 4 any technology solution must also be evaluated not only on the functionality itself, but the compliance in the embedded processes and the training of the user to utilise the technology in the way it was designed.

All these factors must be underpinned by a strong legal and ethical foundation. Questions that already exist in relation to e-Disclosure include how data will be collected and processed, concerns about algorithmic bias & false positives and where the acceptable tolerances lie in this space.

The remainder of this section considers several new or recent technological techniques and capabilities identified through the RFI responses and the desktop review that could be utilised to address some of these challenges.

Artificial Intelligence (AI): This is a broad term that encompasses a number of related fields, including machine learning (the ability to predict most likely events to occur) or predictive coding (use of a computer system to help determine which documents are representative of a defined category) and deep learning (pushing the boundaries of understanding what is possible), all of which are used in situations where the task is so complex or varied that is infeasible to develop an algorithm of specific instructions. It involves the use of algorithms and statistical models that enable computer systems to progressively improve their performance on a specific task through the use of sample or training data in order to make predictions or decisions without being explicitly programmed to perform the task. Examples of applications include data mining, image analysis and recognition, face recognition

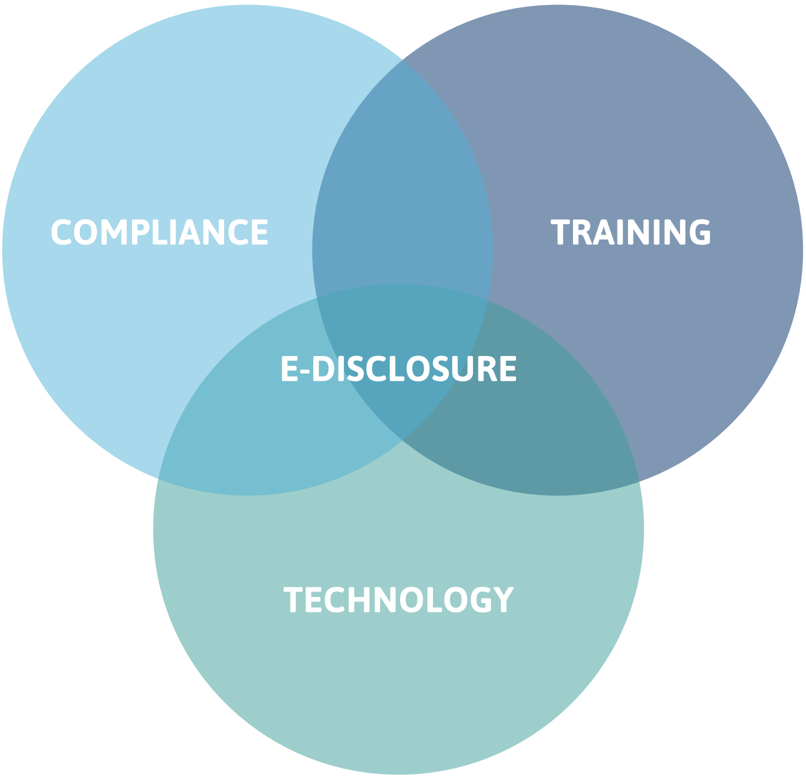


Figure 4 E-Disclosure Technology Considerations

and automation of tasks. There are AI tools with proven open APIs (Application Programming Interface) which would support a modular solution.

- **Advantages:** Industry studies have shown that with the right training, predictive coding achieves better and more cost-effective results than the more traditional, Boolean logic-based approach, which requires humans to give detailed, specifically structured instruction sets for searches.
- **Disadvantages:** Machine learning requires large volumes of training data, and any bias or skew in the dataset will impact the performance. The test applied for disclosure (i.e. assisting the defence case or undermining the prosecution case) is a particularly difficult one for AI to apply. It is also incredibly difficult to identify the factors used to reach its conclusion. Complexity of devices due to encryption and decryption on the fly means that data might not be obvious to the tools.

Advanced searches: As well as key word searches there are a number of search techniques that require less specific inputs ranging from the use of search operators such as wild cards or exact phrase to the use of word clouds to highlight most regularly used words or phrases. Full text search, which requires a text indexing engine, enables searching all text inside any text-based file. There are also advances in video and image search technologies that would increase the efficiency of finding all relevant data.

- **Advantages:** These technologies increase the likelihood of and confidence in finding all relevant data, in particular the word cloud capability may highlight terms that the user may not have thought to search for, and the video and image search capabilities would reduce the time required to review images and video for the relevant files or sections.
- **Disadvantages:** More expensive than simple search capabilities and manual review.

Alerts: Alerts or notifications are machine-to-person communications of important and / or time sensitive information. The use of alerts and notifications to notify the user when new information or data is available against saved searches or analytics is becoming more widespread to replace, where possible, the requirement for manually repeating the same searches or analytics. Techniques include batch processing which is a scheduled run of pre-scripted jobs, and the use of more novel streaming analytics technology which supports the almost instantaneous automated analysis of data as it is arrives in the system.

- **Advantages:** The use of AI can assist in the identification of what would be of interest and requires less manual input. Manual selection or setting of alerts is still more efficient than repeating the same activity on a regular basis, and this approach is more easily auditable. Compared to streaming analytics, batch processing is a relatively simple and inexpensive option to implement. Streaming analytics is closer to real time supporting more time sensitive situations.
- **Disadvantages:** The procurement and implementation of alerting capabilities is more expensive than a manual individual search and analysis approach, and the use of AI would result in the issues identified in the AI section above.

Cloud Computing: This is the provision of software, applications and storage over the internet, and it is still evolving with companies of all shapes and sizes adapting to this new technology.

- **Advantages:** Cloud computing is probably the most cost efficient for organisations to maintain and upgrade, it can scale as required both in terms of storage and user numbers, and is quick to deploy. Public cloud services also provide a lot of services as standard such as backup and recovery. Key advantages for disclosure occur if the forces use the same cloud to store their data as this will facilitate secure sharing and utilisation of collected digital data across local, regional and national boundaries, as well as reduce duplication.

- **Disadvantages:** Users are reliant on a good internet connection (or intranet if a private cloud) to access cloud. Also, there is often a perceived security risk if a public cloud is used, requiring additional confidence that the provider will keep the information totally secure. In addition, private cloud is significantly more expensive than public cloud. It is expected that it will be necessary to store vast volumes of data.

5.3 Planned Delivery

There are a number of other initiatives that are planning on developing and delivering capability that could support the disclosure process and that should be engaged and aligned within any further investigation into or delivery in support of e-Disclosure. Those that have been identified in this landscape review are summarised below.

National Disclosure Improvement Plan (NDIP): This landscape review is one element of the work managed under NDIP, the next phase of which is planned to focus on:

1. Forging strong local partnerships so that police forces and CPS Areas take responsibility to deliver the changes required at every level;
2. Developing the professionalisation of disclosure as a discipline in every police force;
3. Utilising the opportunities of innovative technological solutions and making these tools available to frontline staff in their work;
4. Ensuring a clear line of sight between local and national expectations to ensure that national changes are embedded and taking effect at a local level;
5. Improving communication between the police, the CPS and the defence, including at the pre-charge stage;
6. Monitoring the impact of improvement measures and measuring their effectiveness in investigations and prosecutions; and
7. Learning the lessons of successes and failures of disclosure in our cases to continuously improve our performance month-on-month and year-on-year.

Focus areas 3 and 5 in particular have clear technology links and implications, and as such are particularly pertinent to the technological scope of this review. The breadth of the scope and potential impacts of work planned or in progress is far reaching. As previously described the remit of the NDIP is to identify the necessary activities and coordinate, which will oversee alignment and deduplication of any activities with implications for e-Disclosure.

Digital Policing Portfolio: The Digital Policing Portfolio is a national delivery organisation set up by the National Police Chiefs' Council (NPCC) to deliver the 'Digital Policing' strand of the Policing Vision 2025 focused on developing nationally consistent services, standards and capabilities, in order to:

- Reduce duplication of effort and spend that would occur if all forces developed their own solutions;
- Consolidate learning and share knowledge so all forces benefit; and

- Reduce the 'service lottery' whilst enabling local tailoring and identity of policing services.

The Portfolio is made up of three programmes:

- **Digital Public Contact (DPC):** will change the police's relationship with the public by introducing new intuitive online contact and other services to make policing easier to navigate and more accessible for the public.
- **Digital Intelligence & Investigation (DII):** will enable the police to protect the public by improving forces' digital capabilities to prevent and detect crime and build on those capabilities for future technological advances. This programme's scope includes development and implementation of a national Information Handling Model (IHM), as well as supporting analytical capabilities.
- **Digital First (DF):** will facilitate better working and information sharing between policing and its criminal justice partners. This programme's scope includes the development and delivery of a Digital Evidence Transfer Service (DETS), a Digital Case File (DCF) and supporting implementation of the Two-Way Interface (TWIF) between the criminal justice system and police systems.

National Data Analytics Solution (NDAS): This programme was established in West Midlands Police to investigate the possibility of extending a local strategic project it had funded, known as Data Driven Insights (DDI), which it believed could be scaled nationally. It is a proof-of-concept with the ambition of providing a new scalable and flexible analytics capability to UK law enforcement using advanced analytics to deliver insights to partners on agreed high priority operational and organisational issues. NDAS plans to do the following:

- Introduce a new shared, central data and analytics capability that is aimed and directed proportionately by participating UK law enforcement agencies.
- Provide law enforcement agencies with reporting and support to action insights generated to create more evidence-based local interventions.

Summary: A mapping of which of the key capability requirements these specific initiatives might support is detailed overleaf.

KEY CAPABILITY REQUIREMENTS FROM THE BUSINESS PROBLEM STATEMENTS	DPC	DII	DF	NDAS
1. Nationally consistent data standards			X	X
2. Nationally consistent data formats			X	X
3. Nationally consistent data indexing and cataloguing		X		X
4. Nationally consistent or compatible data enrichment capability				X
5. Nationally consistent or compatible data acquisition and ingest techniques	X			
6. Nationally consistent or compatible data storage infrastructure			X	
7. Nationally consistent or compatible search				X
8. Nationally consistent or compatible analytics capabilities				X
9. Nationally consistent or compatible summary visualisation capability for digital material				X
10. Nationally consistent or compatible data and material sifting and filtering capability				X
11. Nationally consistent or compatible and auditable data access management			X	
12. Nationally consistent and auditable data management and standards		X	X	X
13. Nationally consistent or compatible capability for sharing digital material within and between forces				X
14. Nationally consistent data analytics capabilities				X
15. Cross force data access capability				X
16. Cross force search capability				
17. De-duplication across disparate storage			X	X
18. Capability for sharing digital material with prosecution and defence			X	
19. Capability for sharing analysis of digital material with prosecution and defence			X	

Recommendation: The planned delivery initiatives reviewed above are a subset of the planned or ongoing work relating to e-Disclosure across policing identified during this landscape review. Further work is required to identify any other initiatives to enable deconfliction and deduplication where possible.

6. Gap Analysis

The analysis undertaken in this review reinforces the key capability requirements identified from the business need statements. It should be noted that the technology landscape section is limited to the technologies identified in the RFI responses and additional interviews with technology providers and disclosure SMEs, and three strategic funded initiatives that are more than likely to be a subset of currently funded related work. However it has allowed the first stage of a gap analysis as well as recommendations for next steps. These are captured below:

Review: There are a number of tools identified that appear to provide a good level of capability, providing the material has been imported into a system and is easily found for review. The number of tools does however highlight the lack of a national solution and consistency of approach.

- The consistent extraction, import or ingest of material is critical to e-Disclosure. Process or procedural improvement is out of the scope of this review but is being considered by the wider NDIP.
- This capability is a more general requirement for the investigation process with some e-Disclosure specific requirements including the capture of the evidential audit trail for electronic material. The Digital Case File work in the scope of the DF Programme may also deliver supporting capability. i.e. it will not assist with the review, only with the recording of the findings of the review.
- Recommendation: Further investigation of these tools and any others not identified in this review, along with the work undertaken on the Digital Case File part of the DF Programme and any other relevant nationally funded initiatives should be undertaken to identify if there is a preferred solution the rollout of which would support a consistent approach to e-Disclosure.

Search: The tools identified provide some capability, however the range highlights the lack of consistent, efficient and effective ingest or import of electronic material that is key to the identification of all relevant electronic material for e-Disclosure, as well as the lack of a national solution and consistency of approach.

- The consistent import or ingest and storage of material is increasingly important to ensure that all relevant material can be found quickly with the rapidly expanding volume of material to be considered. This is relevant not only within a force but across forces as material may have been captured by other forces that is relevant to the case in question.
- This capability is a more general requirement for the investigation process with some e-Disclosure specific requirement. This review has not identified any related planned delivery.
- Technology is advancing in this area with advanced search capabilities, AI supported data mining, and the potential for alerts on saved searches which would support the requirement to keep disclosure under review throughout the life of a case.
- Recommendation: Further investigation of these tools and any others not identified in this review may identify a preferred solution the roll out of which would support a consistent approach to e-Disclosure. Consideration of advancing and new technologies that could provide an enhanced solution should also be included in this investigation.

Analysis: Similar to search, the tools identified provide some capability, however the range highlights the lack of consistent, efficient and effective ingest or import of electronic material that is key to the ability to perform effective analysis and identify links or combinations of material relevant for disclosure in policing. It also highlights the lack of a national solution and consistency of approach.

- The consistent import or ingest and storage of material is even more important for analysis as it supports the enrichment of data leading to an increased ability to find links and identify combinations of material relevant for e-Disclosure.
- Technology is rapidly expanding in this area, in particular with AI advances, but there are initiatives with a broader remit in this area that should include e-Disclosure use cases. The DII programme has analytical capabilities in its scope as well as enabling aspects such as national IHM and digital material storage requirement standards, and the NDAS programme which is particularly focussed on analytics.
- Recommendation: There are a number of aspects across the identified related initiatives that have analytical capabilities and technologies in scope. These should be engaged with, along with any other related funded work to ensure that the needs of e-Disclosure are being considered.

Record output of review, search and analysis: Although there are capabilities that provide an audit trail of searches and acquisition activities, this review has not identified any technology that particularly supports the effective and efficient capture of an audit trail of findings and conclusions with any supporting reasoning. This is related to the work being undertaken by Digital First regarding 'Digital Case File'

- The conclusions to be made and recorded here require understanding of any handling caveats or sensitivities of the material which should be captured in the indexing or cataloguing of the material, the completeness of the evidential audit trail, as well as the ability to effectively reference or link to the data so that it can be easily found.
- The indexing and cataloguing aspect that supports this activity is being considered under the DII programme scope that includes the development of a national IHM (Information Handling Model), and digital material storage requirement standards. The only initiative identified that may be considering the Record aspect of the process is the NDIP.
- Recommendation: Further engagement with national programmes and NDDB, as well as any other related funded work, to ensure that the recording requirements of e-Disclosure are being considered.

Assess: The technologies identified against this stage in the process are used to view the material or redo or review analysis that supports the relevance of the material for disclosure.

- Key to the efficiency of this activity is the ability to quickly view / review the material and understand any sensitivities or handling caveats that need to be considered.
- The indexing and cataloguing aspect that supports this activity is part of the DII programme scope that includes the development of a national IHM.
- Recommendation: Further engagement with the DII Programme, as well as any other related funded work, to ensure that the e-Disclosure assessment requirements are being considered.

Record (Disclosure Schedule and Disclosure Management Document (DMD)): Technology can support this through the automatic generation of required documentation based on information captured in the previous Record stage. Only one technology has been identified in this review that supports this activity. Once again this is highly relevant within the development of a Digital Case File.

- Recommendation: Further investigation of this tool and any others not identified in this review may identify a preferred solution the rollout of which would support a consistent approach to e-Disclosure.

Share: Technologies that support this activity have been identified in this review that appear to provide a good level of capability, and the DF Programme is also delivering a DETS and supporting the rollout of TWIF to those forces that have not already adopted this. A DF Landscape Review (2016) found that most England and Wales Police Forces still owned their digital storage in-house. Analysis identified that forces had multiple and often disparate systems with varying business processes and backup systems and little progress had been made in the area of transfer or accessibility of data. Since 2016, a number of forces have put in place solutions for the sharing of multimedia evidence (approximately 12, with more with plans to do so). These have primarily been focused on sharing of BWV, as a result of sharing solutions being offered by the manufacturers of the cameras themselves.

- Recommendation: Further investigation of the existing capabilities including the work under DF to ensure that any e-Disclosure specific requirements are being met.

7. Recommendations and Suggested Next Steps

This section presents the recommendations of this review, a hypothesis on the potential solution, and suggested next steps to address the identified gaps and recommendations.

Technology Landscape Recommendations: The recommendations made as part of the Technology Landscape section are as follows:

- **Current Technology in Policing & Legal profession:** Further work is required to identify other relevant technologies currently in use in policing and both criminal/civil legal profession to assess their capability against the requirements.
- **Planned Delivery:** Further work is required to identify any other funded planned or ongoing initiatives to enable deduplication of effort and identify any gaps.

Gap Analysis Recommendations: Based on the current technologies and planned deliveries identified and reviewed in this report, the recommendations made in the Gap Analysis are as follows:

- **Review:** Ongoing investigation of these tools and any others not identified in this review, along with the other relevant nationally funded initiatives, should be undertaken to identify if there is a preferred solution the rollout of which would support a consistent approach to e-Disclosure.
- **Search:** Further investigation of these tools and any others not identified in this review may identify a preferred solution the role out of which would support a consistent approach to e-Disclosure. Consideration of advancing and new technologies that could provide an enhanced solution should also be included in this investigation.
- **Analysis:** There are a few aspects across the identified related initiatives that have analytical capabilities and technologies in scope. These should be engaged with, along with any other related funded work to ensure that the needs of e-Disclosure are being considered.
- **Record output of review, search and analysis:** The NDDB should continue to engage with national programmes and as well as any other related funded work, to ensure that the recording requirements of e-Disclosure are being considered.
- **Assess:** Continued engagement with the DII Programme, as well as any other related funded work, to ensure that the e-Disclosure assessment requirements are being considered.
- **Record (Disclosure Schedule and Disclosure Management Document (DMD)):** Further examination of the tools (along with the work undertaken on the Digital Case File part of the DF Programme) and any others not identified in this review, may identify a preferred solution the role out of which would support a consistent approach to e-Disclosure.
- **Share:** Supplementary investigation of the existing capabilities including the work under DF to ensure that any e-Disclosure specific requirements are being met.

Hypothesis: Given the range of capabilities required and the cross-cutting nature of disclosure across policing, the most likely solution to the shortfalls is the rollout of a number of technologies, some currently in use and some new, with common APIs, linked together where possible with a common user interface. This would enable a modular approach to the provision of capability with a full range of advanced features, including audit regime, data analytics and search technology. It would also allow for the agile replacement of out dated technologies, and provide the opportunity to keep up with technological advances, as appropriate.

Whilst being cognisant of the necessary differences between forces and in priorities, this rollout should be as wide as possible, and scalable, to encourage consistency in both process and technology across policing to enable better coordination.

The most important parts of the technical solution are likely to be the supporting technology, the common or compatible storage, standards, indexing and cataloguing. Without these the key capabilities of review, search and analysis (which also apply across the rest of the investigation process) cannot be efficient or effective, particularly between forces.

Next Steps: Based on the business challenges and statements of need highlighted in this review, as well as the identified gaps and associated recommendations, the suggested next step would be to assess the above hypothesis as part of an e-Disclosure Outline Business Case that will:

- Conduct more in-depth reviews with representative police forces, including:
  - Capturing the 'as is' process
  - Supporting technologies already in use, and
  - Supporting any other related funded initiatives;
- Engage with the related policing or government initiatives, pilots, proof of concepts to ascertain whether they are addressing any e-Disclosure requirements pertinent to their scope to de-duplicate effort, identify any gaps and seize any opportunities for collaborative working.
- Identify and assess potential options to deliver against the e-Disclosure requirements that have no other identified delivery mechanism.
- Conduct assessments of existing proof of concepts/pilots to select a preferred solution(s) and identify the funding to support the delivery of an e-Disclosure solution(s) that addresses the key business needs and capability gaps whilst delivering the required business outcomes and benefits.

Visit our Knowledge Hub pages
https://knowledgehub.group/group/digital-policing-portfolio-dpp

On the NPCC website
www.npcc.police.uk/NPCCBusinessAreas/ReformandTransformation/Digitalpolicing.aspx

Follow us
@UKDigitalPol @DIIPolice
www.vimeo.com/digitalpolicing