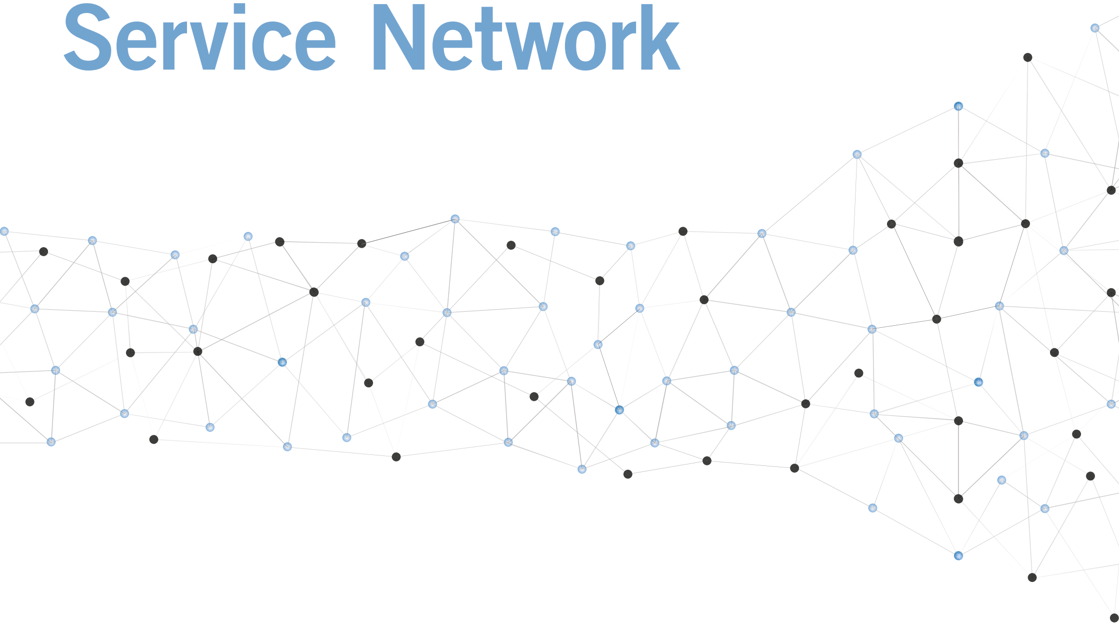
Leeds University
Business School

UNIVERSITY OF LEEDS

Mobile Technology in UK Policing and the Emergency Service Network



March 2018

World Ranked – Triple Accredited – Award Winning

EFMD EQUIS ACCREDITED

AACSB ACCREDITED

ASSOCIATION OF MBAS ACCREDITED

E·S·R·C
ECONOMIC
& SOCIAL
RESEARCH
COUNCIL

EPSRC
Engineering and Physical Sciences
Research Council

Acknowledgements

The Authors would like to thank the members of the project advisory board for their guidance and support:

Steve Whatson
Deputy Director, Emergency Service Mobile Communications Programme (ESN), The Home Office

Dr Nigel Brown
Lead for Resilient ICT Strategy, Cabinet Office

Ian Readhead
Chief Executive, ACRO and National Director of Information

Martin Wyke
Chief Executive, The Police ICT Company

Teresa Ashforth
National MoPI Project, Durham Constabulary

Veronica Scott
Director, Cityforum

Catherine Owens
Evidence and Evaluation Advisor, College of Policing

David Robinson
Business Development Manager, Motorola Solutions

Jeni Jacques-Williams
Digital Solutions Manager, Bluelightworks

With thanks to Bob Larrivee, Vice President and Chief Analyst, AIIM Market Intelligence for giving permission to use AIIM's 2015 data.

We would also like to thank the police forces that co-operated in support of this project. This work has been supported by an Impact Acceleration Award funded by the ESRC and EPSRC. Opinions of points of view expressed are those of the authors.

Report published in March 2018 by the AIMTech Research Centre, Leeds University Business School, University of Leeds, UK.

Citation

Allen, D.K., Norman, A., Williams, S.C., Gritt, E., Forsgren, E., Shaw, N. (2018) Mobile Technology in UK Policing and the Emergency Service Network. Leeds University Business School, University of Leeds, UK.

ORCID provides a digital identifier for researchers.

Professor David K. Allen: orcid.org/0000-0002-8098-6214
Dr Alistair Norman: orcid.org/0000-0002-3229-4360
Mr Simon C. Williams: orcid.org/0000-0003-0160-0457
Mrs Emma Gritt: orcid.org/0000-0002-2369-4928
Ms Emma Forsgren: orcid.org/0000-0001-9227-7821
Dr Nicky Shaw: orcid.org/0000-0002-2799-3634

Contents

Tables and Figures

Executive Summary

This report presents data gathered between 2016 and 2017 on the use and the deployment of devices and the capabilities they provide to Police Forces. We also explore the preparedness of Forces for the Emergency Services Network (ESN). Where possible we present comparative data from similar survey work undertaken in 2004 and 2006 and data gathered from other sectors. The key findings from the research are as follows:

- In 2006, 75% of Forces reported active developments of mobile data. By 2017 UK police services had made significant investments in mobile technology with over 224,455 mobile devices deployed, indicating a more than tenfold increase since 2006. This stands as a significant capital investment in technology and commitment to existing systems which either draw information from mobile devices or send information to them.

- There is a diverse and fragmented landscape of mobile technology deployment as Forces have taken different decisions about the selection and use of laptops, smart-phones and tablet devices.

- For Response and Patrol staff, ‘community’ are the largest single user group for mobile data, being provided with car-fit devices, tablets and body-worn video. Smartphones are now deployed across roles and laptops are deployed to either officers with a specialist role or a management role.

- Forces are deploying multiple devices to support a single role, indicating that a single device cannot satisfy the information needs of some policing roles.

- There is some evidence to suggest that UK police services are providing greater capability for data processing and systems access on mobile devices than comparator private and public sector organisations.

- Forces place emphasis upon purchasing apps from software vendors, using off the shelf apps or buying apps from third parties.

- A small number of Forces are adopting practice from the private sector and allowing officers to choose their own device, or use their work device for appropriate personal use.

- Forces are unsure of ESN’s capabilities, and sceptical about the delivery of the system to the planned timescale.

- 70% of Forces indicate that they will aim to do things differently as a result of ESN.

- A number of Forces have indicated that they will not be ESN compliant on the basis of their current technology configuration. Only 28% of Forces indicated that they used Android as a key operating system.

- A number of Forces have engaged in risk mitigation activities (moving to suppliers that they felt would be ESN compliant) or risk syndication (forming strategic alliances with other Forces following a similar development path).

- Forces are engaging in more collaborative development of systems based on either geographical proximity or the use of similar systems.

- The delivery of ESN does not align with the infrastructure or investment decision of forces of forces with very significant existing implementation of mobile data being within the first transition groups.

Introduction

This is the first of three reports exploring the use of mobile technology in UK police services. In this, the first of the reports, we focus on the devices and capability they provide to the Forces. We also explore the preparedness of Forces for the Emergency Services Network (ESN). This is, perhaps, a particularly opportune point to explore this topic as ESN is rolled out

To undertake this work, we have built upon earlier research projects undertaken for PITO in 2004 and PITO/NPIA in 2006. Where possible we have provided comparative data to allow a longitudinal view of development. Where this has not been possible we have endeavoured to provide comparative data with other sectors. After the closure of the PITO and the NPIA the reports from the 2004 and 2006 studies were embargoed and therefore not published. The research team would like to thank the Home Office for releasing this data and allowing us to use it in these reports.

This report starts by reviewing the methodologies used in the 2004, 2006 and 2017 studies. We then explore the scope of deployments in the UK, describing the type and number of devices deployed. We then turn to the type of devices delivered to different policing roles, the capability of the devices delivered and the development of systems and approaches to the provision of mobile devices. We conclude by discussing police service perceptions of ESN.

Methodology

The three studies referred to in this and the subsequent reports were undertaken as independent research projects. In our 2004 study interviews of groups and/or individuals were conducted in thirteen Forces, face to-face interviews were conducted in a further seven Forces and telephone interviews were carried out in the remaining Forces in England and Wales. In addition, visits and or telephone interviews were made to hardware and software suppliers and to telecommunications providers. We also interviewed IT staff and senior officers involved in the deployment of technology and where possible also interviewed users.

The study was intended to be qualitative because we were specifically requested to collaborate with a separate project being undertaken within PITO which would gather quantitative data. No attempt was made systematically to collect quantitative data other than for illustrative purposes. In our 2006 study telephone interviews were conducted with all Forces. Site visits were also undertaken in the following 11 police services:

1. Merseyside
2. Strathclyde
3. West Yorkshire
4. Lancashire
5. Thames Valley
6. British Transport Police
7. North Wales
8. Surrey
9. West Midlands
10. Metropolitan Police
11. Bedfordshire

For the 2017 study we built upon the question sets used in the 2004 and 2006 studies to develop two semi-structured questionnaire sets, one focussing upon the technology perspective (22 questions) and one focussing upon the operational perspective (18 questions). Information was collected via semi-structured telephone interviews using a mix of qualitative and quantitative questions. All UK terrestrial Police Forces (with the exception of PSNI) were contacted in advance to allocate the necessary time and identify the correct people to speak to during the interview process. The research aimed to obtain two separate interviews per Force with very different perspectives – a technology perspective and an operational perspective. In total, this presented the opportunity to gain up to 88 interviews.

Overall response rates were very high: 100% of UK terrestrial Police Forces (44 in total) were consulted in this research by interviewees reflecting views of their own Forces or in a small number of cases, multi-Force or tri-Force perspectives where such technological or operational arrangements existed. When considering the response rates gained for both technology and operational perspectives, a 96% response rate was gained, with 84 of the 88 potential Force interviews covered.

Type and Number of Devices

In 2004, Forces across the UK were piloting and using a range of different devices and applications, often in small numbers, and in some cases deploying different types of technology to support the same work process in parallel. Twenty-one Forces were running mobile data projects, and fourteen Forces were running pilots or proof-of-concept implementations. Seven Forces reported that they were inactive, however, a number of these indicated that they were planning to implement systems. Innovative Forces identified included West Yorkshire Police with its widespread deployment of early forms of Personal Data Assistants (Grapevine) and then deployment of Blackberry devices, Derbyshire Police Force with Apple Newton computers, Surrey Police Service who provided access to a wide range of applications on its web based Remote Officers and Vehicle Environment (ROVER), Sussex Police focusing on an in-car system using Petard Datex units running APD software with Transcomm UK Ltd providing a bearer. Other notable Forces included North Wales Police Service which delivered to Compaq IPAQ 39 series (with Microsoft Pocket PC), looped to a Sony Ericsson phone and the Metropolitan Police Service Personal Data Terminals using the Panasonic CF-P1.

Two years later our 2006 study revealed that over 75% of the Forces in the UK indicated that they had active developments and deployments of mobile data. The number of devices deployed remained, however, relatively small with approximately 21,629 devices deployed. At this point the largest number devices deployed were Airwave Tetra radios with a limited data capability and in-car mobile data terminals. In 2006 PDAs (usually O2 XDAs) using GPRS were used in some Forces to provide access to key systems such as PNC, Intelligence, e-mail and personal management. Blackberries were used primarily as push e-mail devices but also, in more ambitious applications, providing access to a range of other systems such as the Force Intranet, PNC and Warrants with the aim of providing a paperless end to end system, complete with images. Table 1 below provides a description of the type and number of mobile devices deployed.

Device Type, 2006	Number of Devices
Radio Handset (with data capability)	7,322
Mobile Data Terminal	6,643
Blackberry	3,633
PDA	2,550
Laptop	1,447
Digital Pen	34
Total	**21,629**

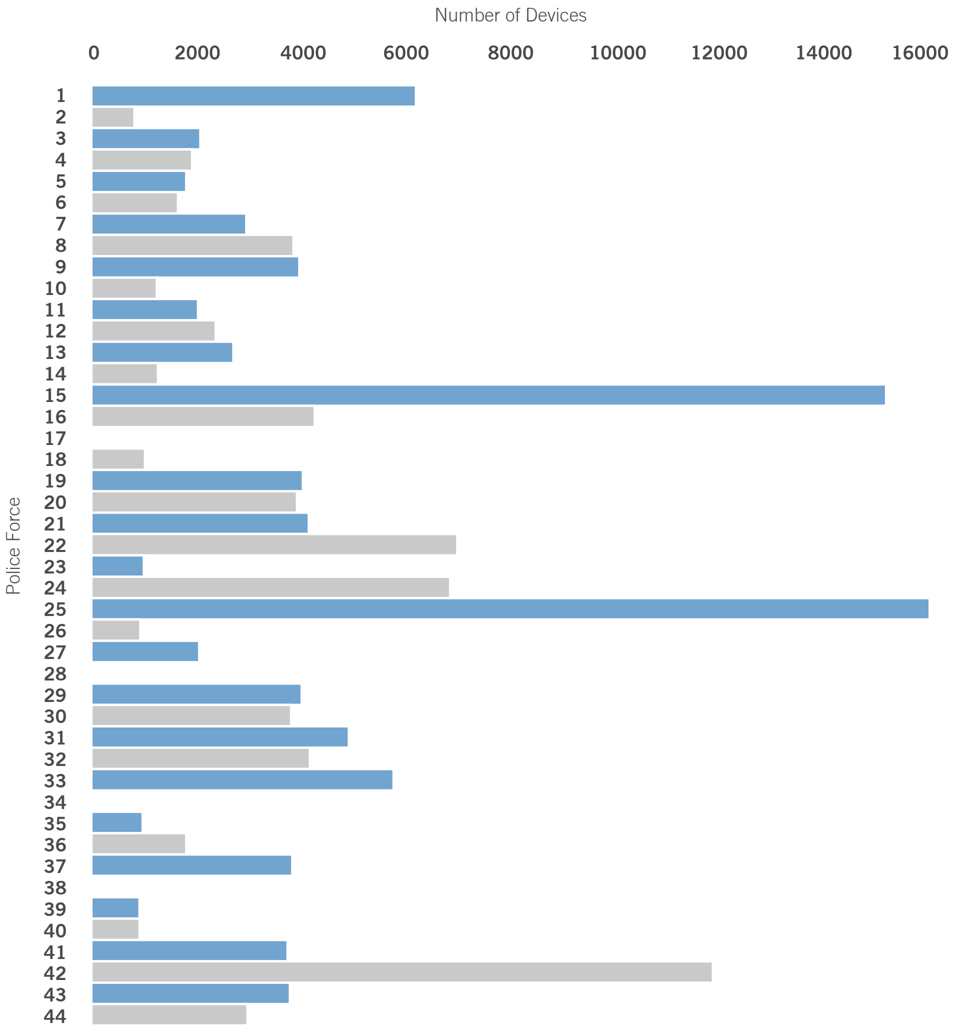
Table 1: Type and number of mobile devices deployed in UK Police Forces, 2006

In 2017 our research indicates that the number of devices has increased significantly with Forces reporting over 224,455 devices deployed (Table 2). This figure, however, must be treated as an indicative figure as in some Forces the respondents were unable to provide a precise number of devices deployed.

Device Type, 2017	Number of Devices
Smart Phones	106,223
Laptops	41,845
Tablets	33,262
Body worn video	42,160
Car fit devices/ MDT	215
PDA	750
Total	**224,455**

Table 2: Type and number of mobile devices deployed in UK Police Forces, 2017

The largest user of mobile data systems was the Metropolitan Police Service. Usage, however, varied significantly from Force to Force. Graph 1 below illustrates the number of mobile devices in UK Police Forces and demonstrates that use is unevenly distributed. This does in part reflect the very different sizes of UK police services, however, it also reflects the fact that Forces have taken different investment decisions.



Graph 1: Total number of devices, UK Police Forces 2017 (excluding the Metropolitan Police)

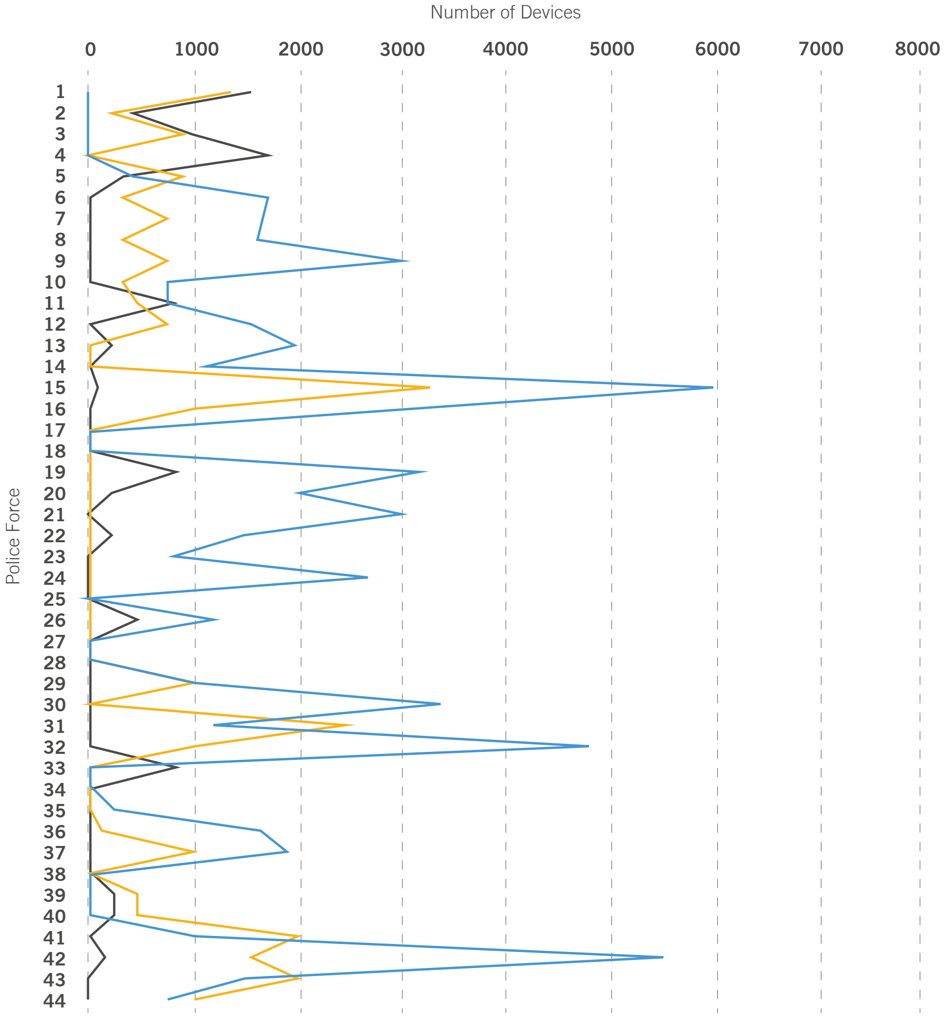
Mobile Data Access Device Types by Force, 2004

Force	Device type					
	MDT	Laptop	Tablet	Blackberry	PDA	Total
Avon & Somerset		Y				1
Bedfordshire						
Cambridgeshire	Y	Y				2
Cheshire						
City of London		Y				1
Cleveland	Y				Y	2
Cumbria						
Derbyshire		Y			Y	2
Devon & Cornwall		Y			Y	2
Dorset	Y	Y				2
Durham		Y			Y	2
Dyfed Powys	Y	Y				2
Essex		Y	Y		Y	3
Glos						
GMP	Y	Y			Y	3
Gwent	Y					1
Hampshire	Y	Y	Y			3
Herts		Y			Y	2
Humberside		Y	Y	Y		3
Kent	Y				Pilot ended	1

Lancs	Y	Y	Y	Y	Y - larger pilot due	5
Leicestershire		Y				1
Lincolnshire	Y					1
Merseyside		Y				1
Metropolitan Police	Y				Y - Pilot	2
Norfolk						
Northants	Y	Y	Y			3
North Yorks						
Northumbria	Pilot ended	Y				1
North Wales	Y		Y		Y 200 units	3
Notts		Y	Y			2
South Wales		W/d			W/d	
South Yorks		Y	POC due	Y	POC due	2
Staffs		Y				1
Suffolk						
Surrey	Y	Y	Y	Possible pilot	Pilot	4
Sussex	Y				Y covert only	2
Thames	Y	Y		Y	Y	4
Warwickshire		Y				1
West Mercia		Y				1
West Midlands	Y	Y	Y			3
West Yorks	Y	Y	Y	Y	Y	5

Table 3: Mobile device types used in UK Police Forces, 2004

Graph 2 below depicts the usage of smart phones, laptops and tablets by individual Forces in 2017. This indicates that Forces continue to deploy different devices in parallel, however, that different Forces take very different approaches to selection and provision of devices. While the key device for many Forces is seen in the rise of smartphones, a number of Forces are also deploying laptops and tablets. Dedicated, single-use in-car terminals are declining in number and tend to be focused on roles such as traffic where the role supports the use of such a device.



Graph 2: Smart Phone, Laptop and Tablet use, UK Police Forces 2017 (excluding the Metropolitan Police)

Roles and Devices

In our 2004 and 2006 studies we analysed the deployment of technology according to work roles. Our 2006 study specifically indicated that community officers saw benefit from using handheld devices with tablet and laptops also useful in this role, especially when officers work from a fixed base. Response officers operating double-crewed tended to prefer in-car terminals. Single-crewed response officers tended to prefer handhelds as they were unable to use the in-car terminal while driving. Traffic officers tended to prefer in-car units. Managers and supervisors tended to see clear value in handhelds such as Blackberrys' which allowed access to Personal Information Management (PIM)and e-mail applications. Laptops were also popular with managers but these are primarily used as nomadic (i.e., taken from place to place) rather than mobile (i.e., while working on the move). Specialists such as Scenes of Crime Officers tended to prefer laptops with full size screens and these tended to be 'toughened' devices to cope with the rigours of field use as opposed to use of laptops issued to other roles. In our 2017 study we focused on car-fit devices, smartphone, tablet, laptop and body-worn video.

The results suggest that the Patrol: Response and Patrol: Community are the largest single user group for mobile data being provided with car-fit devices, tablets and body-worn video. Smartphones are now deployed across roles and laptops deployed to either officers with a specialist role or a management role. Twelve Forces indicated that they were piloting body-worn video or tablets. The results indicate Forces deploying multiple devices to support a single role.

Car-Fit Devices

In the 2004 and 2006 studies we focused on the use of Mobile Data Terminals (MDT). In our 2017 study, however, we used the term car-fit device to indicate an expanded use of a range of technologies which could be used within the police car to inform the officer or gather data on work activity. As expected the responses indicated that the primary use was by patrol officers either acting as response officers or community officers (Table 4).

Activity	Pilot	Deployment	Unsure	Total
Patrol: Response	2	28	0	30
Patrol: Community	2	14	0	16
Volume Crime (detective)	0	3	1	4
SOCO	1	4	1	5
Supervisors / Sergeant	0	6	0	6
Middle Managers / Inspector	0	3	1	4
Executive Managers / Chief Inspector	0	4	1	5

Table 4: Car fit devices used by UK Police Forces, 2017

It is clear, however, that a number of Forces view police vehicles as a key part of their mobile strategy moving beyond provision of data to the officer in the vehicle through an MDT and describing them as a platform for sensors from which they can pull and then integrate data to improve performance and as a nodal point in mobile networks. One of our respondents noted:

> “*It is amazing that we didn’t have it before when you see what people do with it – it is a game changer. In the next 12 months we will have more of a converged aspect, so our car fleet, telemetry and ANPR – there is a big piece of work with our car fleet which will enable them to be mobile hotspots…*”

Smartphones

Our 2017 study indicated that smartphones are now not only deployed for patrol officers, however, are deployed in a wide variety of roles (Table 5). They have, in effect, become the dominant form of mobile technology within most settings and it does not appear likely that this will change in the near future. The takeup of newer technologies (such as wearables) is very low and advances in smartphone capabilities mean that their use is likely to continue.

	Pilot	Deployment	Unsure	Total
Patrol: Response	2	34	0	36
Patrol: Community	0	34	0	34
Volume Crime (detective)	0	23	0	23
SOCO	0	25	0	25
Supervisors / Sergeant	0	35	0	35
Middle Managers / Inspector	2	36	0	38
Executive Managers / Chief Inspector	2	37	0	39

Table 5: Smartphones used by UK Police Services, 2017

Laptops

Laptop use again varied considerably from Force to Force with some providing them to community and response officers, however, the majority deploying them to middle managers/ inspectors and above (Table 6). The numbers of these devices in front line operational use are falling although some operational users have a strong attachment to the laptop format. This tends to be role-associated with statement taking being an example of a function that users see as being facilitated by access to larger screens and, crucially, what users describe as a 'proper' keyboard.

	Pilot	Deployment	Unsure	Total
Patrol: Response	2	15	0	17
Patrol: Community	0	14	0	14
Volume Crime (detective)	0	25	0	25
SOCO	0	28	1	29
Supervisors / Sergeant	0	24	0	24
Middle Managers / Inspector	0	34	0	34
Executive Managers / Chief Inspector	0	36	0	36

Table 6: Laptops used by UK Police Services, 2017

Tablets

Tablets were deployed less frequently than the other technologies identified (Table 7). These seem to be used primarily by patrol officers or Chief Inspectors or above. A minority of Forces have very significant tablet deployments and these are usually in conjunction with other devices.

	Pilot	Deployment	Unsure	Total
Patrol: Response	1	18	0	19
Patrol: Community	0	18	0	18
Volume Crime (detective)	2	8	0	10
SOCO	4	8	0	12
Supervisors / Sergeant	2	6	1	9
Middle Managers / Inspector	2	9	1	12
Executive Managers / Chief Inspector	1	19	0	20

Table 7: Tablet use by UK Police Services, 2017

Body Worn Video

The survey data indicated that body worn video is being rolled out primarily to patrol officers (Table 8). The trend for this technology to be adopted and used is clear although there are detail differences in deployment patterns and the management of the Body Worn Video equipment. Personal issue is becoming the norm for this technology in many, although not all, Forces.

	Pilot	Deployment	Unsure	Total
Patrol: Response	5	28	0	33
Patrol: Community	4	20	0	24
Volume Crime (detective)	0	8	0	8
SOCO	1	3	1	5
Supervisors / Sergeant	1	14	0	15
Middle Managers / Inspector	0	4	0	4
Executive Managers / Chief Inspector	0	2	1	3

Table 8: Body worn video used by UK Police Services, 2017

Capabilities on Device

Access to a device, while important, is only one step towards enabling mobile work. Of equal, if not more, importance is the capability-set enabled on the device. A perception in UK policing is that officers are falling behind other types of employment and the devices that they are issued with have less capability. To explore whether or not this view had any substance we replicated an element of study by the non-profit Association for Information and Image Management (AIIM) in late 2015 (AIIM 2015). The results are show in Table 9 below:

	Police Forces (2017; n=42)	Count	AIIM	Count
VPN access to remote desktop or file share	88%	37	(2015; n=186)	59
Search and view content stored in ECM / DM - browser only	62%	26	32%	52
Search and view content stored in ECM / DM - dedicated app	52%	22	28%	28
Offline content access	74%	31	15%	26
Commenting and editing capability	83%	35	14%	26
Can create content (docs / photos / images) directly into ECM/workflow	81%	34	14%	24
Able to interact with tasks / processes / approval cycles	93%	39	13%	30
Signature sign-off on forms, contracts, or processes	76%	32	16%	22
Camera-scanned forms input (e.g. driving license)	24%	10	12%	12
Mobile e-forms related to on-premises processes (e.g. witness statements / evidence)	74%	31	7%	12
None of these	2%	1	7%	72

Table 9: Monitoring and Evaluation Process to Measure Benefits – Cost and Efficiency

The AIIM survey focused on a small subset of its 80,000 community members and, given its membership is skewed towards the US it can be expected that it would reflect this demographic. The results, however, provide an indication that UK police services are providing greater capability on mobile devices, to some of their officers at least, than other private and public sector organisations. Indeed, the results indicates that Forces collectively if not individually, are providing significantly more capability. We explored this further with the Forces and asked about the applications that they were delivering on mobile devices. The results from this question are displayed in Table 10 below and indicate that Forces were deploying a wide range of applications. In our 2006 survey the most commonly used applications across Forces responding to the survey were: PNC access (23 Forces), e-mail (21), diary access and ANPR (14), Command and Control interaction (11) and intranet access (10).

	Applications deployed on mobile devices, 2017
Forms	38
Social Media	37
Messaging	37
PNC-Police National Computer	37
Images: Still	37
Crime recording	35
Intelligence	35
Stop and search	32
ANPR (Automatic Number Plate Recognition)	28
Duties	28
Electoral roll	27
CAD (Computer Aided Dispatch)	26
Images: Video	23
Road traffic	18
Warrants	18
AVLS (Automatic Vehicle Location Information System)	17
Crime scenes	16
Other (please state)	5

Table 10: Applications deployed on mobile devices, UK Police Forces, 2017

This demonstrates that Forces are deploying devices which allow the submission of data (through forms) and applications which allow communication with citizens or colleagues (social-media, mail) in addition to applications which directly support decision making (such as PNC and Intelligence). Respondents replied to this question by stating 'other' provided a view of the current developments in this area. One respondent pointed out that *"Our mobile solution replicates our desktop so anything that an officer can do in the office, they can do out and about but it would be quite a lot to add"*. Another pointed to a range of reports and forms stating that these included:

> *" A missing person report, a Dial form which is a domestic abuse form, a MARF form, multi-agency referral, stop and search, traffic report, HORT1 which is another traffic report, Section 165 traffic vehicle assessment report, witness statements and crime scene examination. There's a raft of them because obviously we're currently in rollout of mobile data, what I've just gone through, the list I've read to you is nine processes, we've got 30 processes to deliver that we've contracted for, so a raft of other capabilities are coming in the next few months. "*

Only a limited number of Forces were able to confirm whether or their officers could undertake a federated search on mobile devices. Most indicated, of those that were able to respond, that it was available only on desktop machines or that limited functionality was available. The Forces that do provide this capability indicated that this was seen as an important element of provision of data to officers. One noted, for example, that while they currently provided federated search they were *" …starting to develop two federated search systems, one is for federated search on mobiles, that simply takes the name … and does a skim search across a variety of different systems but we're also then working with X … to build a 360 degree picture of your search, so if you search for a location, it will bring a load of information back about that particular position you're in or a particular individual and it will also do things like analyse your spelling and look for different dictionary definitions of how you've spelt names and so on, so it becomes far more of a probabilistic search than a yes/no search."*

Provision of Devices

Bring your own device or choose your own device (BYOD / CYOD) has been described, mainly in the private sector, as providing significant benefits for large organisations in the provision and management of mobile technologies. CYOD has also been conflated in a number of applications with the Company Owned, Personally Enabled (COPE) model of device provision where a work tool can be used for (reasonable) personal use. These benefits of these approaches range from reducing mobile infrastructure costs to reducing the time required for training.

However, a number of concerns have been raised about the approaches, especially in sensitive data settings, including issues related to data governance and security. In order to provide comparative statistics, we utilised a question developed by AIIM (2015) to understand the approach used in UK policing and allow the comparison with the other sectors (Table 11). The data gathered by AIIM provides a particularly conservative estimation of use with only 36% of organisations using CYOD or BYOD. The results, however, indicated that none of the Forces were using a BYOD approach. However, 17% were allowing CYOD.Numerous examples were cited by the respondents reflecting the fact that as Officers use and deploy technology they will uncover and invent new ways of using the technology. The challenge for Forces is to both capture and cascade beneficial new ways of working across the Force while controlling less beneficial or problematic approaches.

	Police Forces (2017; n=41)	Count	AIIM	Count
Successfully introduced and running smoothly	2%	1	(2015, n=219)	22
Working OK, but with some issues	2%	1	10%	44
Getting there, but taking up a lot of support time	7%	3	20%	10
Only available to some staff	0%	0	5%	34
We're just rolling it out now	0%	0	16%	6
We're at planning stage	0%	0	3%	14
We do allow personal use of company-owned (COPE)	17%	7	6%	14
We're sticking to company owned, business use only	7%	3	6%	29
None of these - not allowed	59%	24	13%	17
None of these - there is no stated policy	5%	2	8%	29

Table 11: The progress and success of 'bring your own device' or 'choose your own device', 2017

Development of Systems and Provision of Mobile Devices

In 2017 93% of Forces used mobile applications. This provides one indicator of the extent to which they are allowing access to data through systems designed for mobile environments, rather than browser based solutions. Of equal interest is the way in which they develop and deploy these applications. We asked respondents to indicate how they source mobile context applications. The question we asked replicated one used by AIIM in 2015 with a broad spectrum of public and private sector organisations to provide indicative comparative figures.

The results (shown in Table 12 below) suggest that Forces place emphasis upon purchasing apps from third parties, using off the shelf apps or using a specialist systems integrator. Given the significant number of respondents to the AIIM survey who didn't use apps, or didn't know how they were acquired, comparisons should be seen as indicative only. The data does, however, suggest that Police Services in the UK are more likely to use a specialist systems integrator or buy apps from a third party than other organisations.

	Police Forces (2017; n=37)	Count	AIIM	Count
Develop in-house	27%	10	(2015; n=72; excl. 42 'don't know' or N/A)	13
Develop in-house but using a recognized MDM (mobile device management) / MAM (mobile application management) platform	38%	14	18%	12
Buy apps from ECM (Enterprise Content Management) / BPM (Business Process Management) software vendor	22%	8	17%	14
Buy apps from 3rd parties	68%	25	19%	12
Use a specialist systems integrator	49%	18	17%	6
Use off the shelf apps	54%	20	8%	15

Table 12: Sourcing mobile context applications, 2017 and 2015

Note: Whilst the AIIM data was collected asking respondents to 'tick one response only', it became apparent that for Police Forces in 2017, multiple options were being used. Therefore, this was left as 'tick all that apply' to better reflect the current environment.

Cross Force Collaboration in Mobile Solutions

In 2004 and 2006 cross-force collaboration in the development of mobile solutions was embryonic and basedon sharing of experiences and best practice. By 2017 Forces reported dyadic or multi-partner strategic alliances based on geographic co-location. Equally, they discussed the way in which they had developed strategic alliances based on the use of a common system often supported through technology supplier usergroups. There are, however, significant challenges to the development and maintenance of these relationships. While some Forces indicated that collaborations were working well others pointed to failed attempts at collaboration or issues which created barriers to entry into collaboration.

A key barrier identified by respondents to the development of collaborative development of mobile technologies was the very different technology infrastructure developed and deployed by Forces. Respondents noted that Forces had different systems and technologies and even when they shared a system with other Forces they would find that they had configured their systems in different ways. As one respondent noted:

"Forces being on a different technology stack, e.g. from an operating system to the software we use, also even if there is commonality between the software we use, the way we configure is a very local thing as opposed to a regional or national thing…".

Respondents also noted that the lack of common networks to collaborate on, and a lack of standards for information interchange were also key barriers to collaborative development of systems.

Others viewed the technology not as a barrier itself but as a reflection of other concerns. One respondent articulated this view when they stated *"Technically, there are really no barriers, we can do technically whatever a police force wants to do, we can join networks, we can create a move to single IT systems, technically anything is physically possible. A lot of people could say it's a barrier because it's hard and it takes a long time and there's a load of technical levels but with money, time, effort, you'll get the technology done."*

The respondents indicated that the more significant barriers were related to differing working practices and needs. As one respondent stated:

"I think the cultures within Forces are so different. The operational structure within the Forces, deployment methods, the arrangement for dealing with incidents, the command and control systems, our RMS and everything is different so it's very difficult to make a joint approach to mobile work".

An often cited barrier noted was need for the political will to collaborate:

"The key downfall is the ability of Forces to join upon a single vision about how they're going to operate, who's going to manage what, what the Police & Crime Commissioners are responsible for and how do we all work… together, that's the main barrier to be frank."

Respondents pointed to difficulties in achieving agreement and then further difficulties in maintaining agreements as personnel changed. One respondent noted that:

> *"Most recently, we've gone through a couple of collaboration agreements with regional Forces and where we've fundamentally tripped over is that even though police constables have agreed to work together, Police & Crime Commissioners have muddied the landscape and we've found that they haven't been able to agree with each other because it's them who have the primarily local agenda more than the police constables. So, if you want me to boil it down, it's the way that police Forces work with Police & Crime Commissioners, that's fundamentally been a barrier in our area at least. We could spend an afternoon talking about that!"*

We then asked the Forces to identify the issues that limit the development of national standards for mobile solutions. The respondents pointed to a range of factors the primary one was the lack of resources to develop the standards.
One respondent noted:

> *“Lack of resources doing it is the main one. Since I’m on the group and the majority of the work is being done by people who are already have significant day jobs like myself. So, doing standards as well as doing your own job in force which you are paid to do is very difficult”.*

The respondent also pointed to the different and sometimes conflicting needs of the Forces:

> *“I think you’ve got 43 different organisations all with their own agendas and at different points in the lifecycle and nobody wants to sit there and put the standard together….”*

Emergency Services Network

The new Emergency Services Network is intended to provide UK emergency services with a ‘next generation’ communication system. We asked the Forces if they were planning to do anything different as a result of ESN (Table 13). 70% of the Forces that were willing to respond to this question indicated that they would do so. It must be noted, however, that only 27 Forces were willing to respond to this question.

	%	Count
Yes	70%	19
No	30%	8
TOTAL	**100%**	**27**

Table 13: Are you planning to do anything different as a result of ESN?

A small number of respondents indicated that they viewed ESN as providing Forces with the capability to transform the way in which they work. One respondent noted:

“I think ESN has the potential to completely change the work we work, i.e. every cop on the street with access to mobile data and mobile applications, it brings a huge number of opportunities and potential advantages. I think it is all going to be down to how ESN works and how that integration of an application into the ESN environment is actually realised.”

Despite his positive perspective this respondent, in common with many others, pointed to a degree of uncertainty about what ESN would deliver. A number of respondents indicated that they were both unsure of its potential capabilities and skeptical about the delivery of ESN. The following quotation is typical of the statements made by these respondents:

“Well who knows what ESN is?... Well they’ll tell you that it’s the best thing since sliced bread, but when you deep dive into the technical detail there’s nothing there.”

Forces that were changing as a result of ESN pointed to risk management strategies. One of these was to collaborate with other Forces to share or syndicate risk. A number indicated that the main thing that they would change was that they were moving to Android or to specific vendors to reduce risk and ensure that their mobile operating system was ESN compliant. As one respondent noted:

“We have just brought in a product called X… To do that we need Android. The leverage for that was ESN, because it’s Android based.”

Another noted that:

“The second bit that we’re looking at is the applications that go on those devices. Now, what we’re doing differently … but making sure ..., that they are going down the route of being compliant against the Motorola Lot 2, which is the accreditation of applications on phones, effectively, so that means that whatever we choose for our mobile phone rollout now, will be accredited on ESN or ideally accredited on ESN once the new devices become available effectively”

The respondent also pointed to the different and sometimes conflicting needs of the Forces:

“Very much so, yes, we’ve worked very closely with the national ESN team and our consultants to ensure that our recent investment in smartphones were ESN compliant, [Name Removed] Consulting worked with us on a business case and they’re also linked into the national ESN project and were able to give us information that Android was going to be the first operating system that ESN focused on, which really encouraged us to go down the Android route”

The primary response was, however, that Forces were not sure of the standards that they needed to be compliant with (beyond an Android operating system). The following two respondents provided typical responses:

> “The question I would ask in return is, “what does ESN compliance mean”? There are no guidelines about application about what they have to be, there’s no standard on the app, just an accreditation process that is vague and not defined because they are struggling delivering the actual overall solution. So, I would say it is impossible to say anything is ESN compliant or to understand what that might undertake because the project is yet undefined in terms of the end solution.”
>
> “You tell me what ESN compliant means, nobody knows and I’ll tell you if I’m compliant because nobody knows what the devices are, nobody knows what’s going on with the devices, nobody really knows when they’re going to be deployed, nobody really knows exactly what the network coverage is. So I can tell you hand on heart, we’re absolutely compliant because we don’t know anything about it.”

30% of Forces, particularly those with larger deployments indicated that they wouldn’t be ESN compliant. One stated: “Based on what I understand of the strict regime they’re implementing, my answer would be no. We have a different philosophical model to the very strong limited model that ESN is using.” Another noted “Our biggest worry about ESN is ESN seems to be an Android only solution. The second concern is it is standardising on a mobile device management environment that doesn’t work with Android. We’ve got old BlackBerry and everything else but we’re standardised on X platform…” The most often citied barrier to becoming ESN compliant was use of another operating platform. This could be a significant factor for ESN deployment as our research indicates that a large number of mobile devices used in UK policing are currently on a Windows platform with only 28% of Forces using Android (Figure 1).

A number of Forces indicated that as they already had significant investments and expertise in mobile and the extent to which they would use ESN for data would depend on pricing and flexibility. One Force which indicated that it was intending to be ESN compliant indicated that this decision would be reconsidered once further details were provided:

"I worry that it might be too inflexible and not financially practical to have anything other than national mobile applications based on the ESN platform. We may need to look at something else for anything we look at on a more bespoke basis."

Indeed, a number of Forces indicated that they expected to run ESN compatible devices in parallel with alternative approaches:

"...your officers have your ESN compatible device for radio – push to talk and all the live stuff on there – but we have a separate device that we have much more control over in terms of our apps, potentially it depends on how it all hangs together on cost and capabilities".

What operating systems are being used?

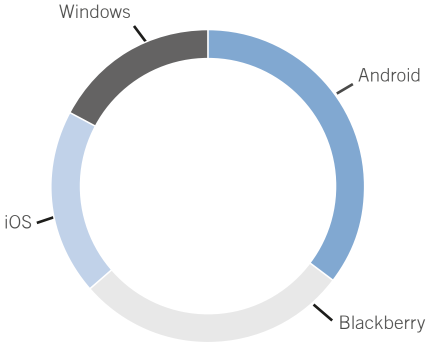


Figure 1: Operating systems deployed on mobile devices, UK Police Forces 2017

Implementation of ESN

Using Home Office information about the implementation of ESN programme (Home Office 2016), it can be seen that implementation is proposed in 12 'Regional Transition Groups' commencing with the North West and ending with the South West. This is illustrated in Figure 2.

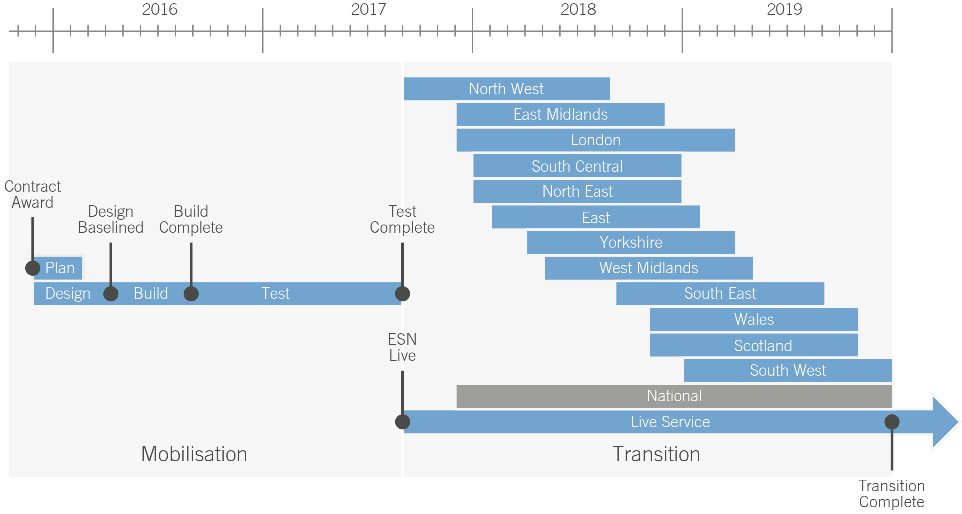


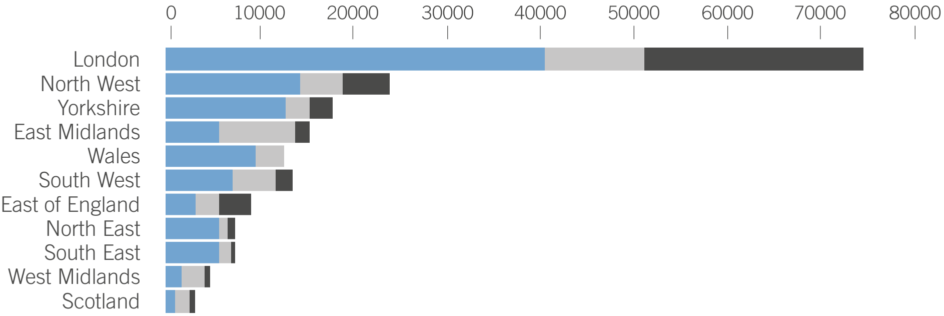
Figure 2: Implementation Plan for ESN (Home Office, 2016)

While we recognize that this plan has been delayed the regional approach to delivery remains. When comparing this to the number of devices in Forces within the regional transition groups (illustrated in Table 14), there is an argument which can be posed whereby the approach to implementation should be changed to target those Forces with the lowest levels of investment and technology hardware infrastructure first.

Regional Transition Groups	Mobile Hardware (2016/17)
Scotland Transition Group	2,700
West Midlands Transition Group	5,260
North East Transition Group	7,025
East of England Transition Group	7,800
South East Transition Group	9,223
Wales Transition Group	12,750
South West Transition Group	16,062
Yorkshire Transition Group	19,190
East Midlands Transition Group	19,865
North West Transition Group	29,830
London Transition Group	95,600
South Central Transition Group	Incomplete Data Set

Table 14: Mobile hardware used in Forces (2016/17)

Graph 3 (below) demonstrates that not only does the volume of investment differ markedly between regions but also the type of technology used varies significantly. Thus, for example, the West Midlands, East Midlands and South West Forces place more emphasis on laptop use than those in Yorkshire or the North West. It is unclear how the roll out plan for ESN will align with the existing infrastructure and the lifecycle of the infrastructure.



Graph 3: Device Type by ESN Region

Conclusion

The research suggests at least a tenfold overall increase in scale and scope of deployments of mobile technologies from our original 2004 study. Police Forces, collectively, are providing greater capability for data processing and systems access on mobile devices than comparator private and public sector organisations. Equally, respondents indicated that a number are collaborating with other Forces on development as part of a wider strategic collaboration or on the use of a common platform. The mobile technology landscape is, however, particularly fragmented with Forces taking different approaches to use and deployment of mobile technologies.

There is widespread concern about the deployment of ESN, lack of knowledge about the capabilities and limitations of the proposed network and devices and scepticism about the benefits associated with moving from existing deployments to ESN as well as the likelihood of adherence to the planned timeline. The current pattern of deployment and use is uneven with some Forces making significant investments, whilst others have been more conservative in their investment strategy. It is, however, clear that there are Forces that already have a significant amount of technology deployed which may not be compatible with ESN; for example, a range of alternative operating systems are being deployed on devices. While there is an articulated desire for the development of national standards and collaborative agreements at a local level there are significant challenges to the development and maintenance of arrangements which allow the development of common systems.

References

AIIM (2015). Mobile & Cloud: Accessing, Capturing, and Processing Content. [Online]. Available from: http://info.aiim.org/mobile-and-cloud Date Accessed: 15.11.2017

Allen, D.K., Norman, A. (2004). Mobile data systems in Police Forces in England and Wales: Final Report. AIMTech Research Group, Leeds University Business School, University of Leeds, UK.

Allen, D.K., Norman, A., Knight, C. (2006). PITO National Data Survey (12th July 2006). [Redacted], AIMTech Research Centre, University of Leeds, Leeds, UK.

Allen, D.K., Norman, A., Williams, S.C., Gritt, E., Forsgren, E., Shaw, N. (2017). Policing, Information and Technology in the UK: A national survey. Leeds University Business School, University of Leeds, UK.

Home Office (2016). Emergency Services Mobile Communications Programme – Spectrum Policy Forum Briefing 14th July 2016. Home Office, London, UK. [Online]. Available from: https://goo.gl/M5qsst Date Accessed: 17.11.2017

Appendix 1: List of Forces Consulted in This Research

1. Avon and Somerset Constabulary
2. Bedfordshire Police
3. Cambridgeshire Constabulary
4. Cheshire Constabulary
5. City of London Police
6. Cleveland Police
7. Cumbria Constabulary
8. Derbyshire Constabulary
9. Devon & Cornwall Police
10. Dorset Police
11. Durham Constabulary
12. Dyfed-Powys Police
13. Essex Police
14. Gloucestershire Constabulary
15. Greater Manchester Police
16. Gwent Police
17. Hampshire Constabulary
18. Hertfordshire Constabulary
19. Humberside Police
20. Kent Police
21. Lancashire Constabulary
22. Leicestershire Police
23. Lincolnshire Police
24. Merseyside Police
25. Metropolitan Police
26. Norfolk Constabulary
27. North Wales Police
28. North Yorkshire Police
29. Northamptonshire Police
30. Northumbria Police
31. Nottinghamshire Police
32. South Wales Police
33. South Yorkshire Police
34. Staffordshire Police
35. Suffolk Constabulary
36. Surrey Police
37. Sussex Police
38. Thames Valley Police
39. Warwickshire Police
40. West Mercia Police
41. West Midlands Police
42. West Yorkshire Police
43. Wiltshire Police
44. Police Scotland

Note: PSNI was not included in the study.