MOTOROLA *SOLUTIONS*

REFORM

Frontline online
Smarter blue light services

Sarah Timmis
Emilie Sundorph
Alexander Hitchcock

MOTOROLA *SOLUTIONS*

March 2018 #Reformbluelights

Frontline online
Smarter blue light services

Sarah Timmis
Emilie Sundorph
Alexander Hitchcock

March 2018

Acknowledgements

Reform

Reform is an independent, non-party think tank whose mission is to set out a better way to deliver public services and economic prosperity. Our aim is to produce research of outstanding quality on the core issues of the economy, health, education, welfare, and criminal justice, and on the right balance between government and the individual.

Reform is a registered charity, the Reform Research Trust, charity no.1103739. This publication is the property of the Reform Research Trust.

Technology will transform public-service delivery. Services citizens use when in greatest need, as victims of crimes, fires or in a medical emergency, should be at the forefront of this. Ambulance, fire and police crews are beginning to use technology on the frontline, and 94 per cent of police organisations recently said the digital agenda tops the list of priorities moving forward.[1] However, services must accelerate the move from simply replicating current administrative processes digitally, to a smarter and more joined-up approach. The Government has committed to this agenda. As Brandon Lewis, then Minister for Policing and the Fire Service, argued in 2016, "technologies…can transform service delivery both for the service and the communities we serve."[2]

The opportunity is great: more efficient, more collaborative, and more responsive emergency services, fit to respond to citizens' needs today and in the future.

Emergency service data

Information silos

Emergency services are swimming in data. For every one of the more than 10 million incidents attended by police, fire and ambulance services every year, information is recorded – on everything from incident details to data on people involved.[3] This is crucial for responding accurately to people's needs. For example, Derek Cartwright, Chief Executive of the North West Ambulance Service, explains that 95 per cent of the service's calls are of an urgent care nature: typically elderly people, with multiple long-term conditions.

Cartwright argues that sending the appropriate available information to ambulances' crews before they arrive at a scene would further improve the position from which crews can intervene and plan a care pathway for their patients. Police forces struggle with incompatible data recording regimes, where simple differences like categories of hair colours can prevent data sharing. Alex Rhodes, a Station Manager at Hampshire Fire and Rescue Service and the National Fire Chiefs Council Lead for Research and Development, says his officers are concerned with the absence of information on risks entering certain homes. Firefighters only get police information if they happen to have police attending incidents with them.

It is no surprise that data sharing between public bodies is notoriously underused. A 2016 study found that there is a culture of risk-aversion when it comes to knowledge-sharing, which is hindering progress.[4] The Chief Constable of Essex Police and the NPCC Lead on Digital Policing, Stephen Kavanagh, argues that some police forces and public-sector parties prefer simply not to pursue innovative data sharing, rather than seeking comprehensive legal advice.

Legality and security of sharing data

Kavanagh also emphasises that in a "post-Snowden world", emergency services – which hold the most sensitive personal information – should clearly communicate the benefits of data sharing, and ensure that all information is handled securely. Research has found that the public accept data sharing if the reason for sharing is clear, such as for direct care purposes,[5] but also that citizens share a general sentiment that the Government does not take the security of personal data seriously.[6]

---

1 New Statesman, *Digital Policing: The Path to 2025* (New Statesman, 2018).
2 Brandon Lewis, 'Speech to APCC & NPCC Joint Summit on Emergency Services Collaboration', Webpage, 18 November, 2016.
3 College of Policing, *College of Policing Analysis: Estimating Demand on the Police Service*, 2015; Health & Social Care Information Centre, *Ambulance Services, England 2014-15*, 2015; Home Office, *Fire and Rescue Incident Statistics: England, April 2016 to March 2017*, 2017.
4 Centre of Excellence for Information Sharing, *Overcoming Cultural Barriers to Information Sharing within Regulatory Services*, 2016.
5 National Data Guardian for Health and Care, *Review of Data Security, Consent and Opt-Outs*, 2016.
6 Office for National Statistics, *The Census and Future Provision of Population Statistics in England and Wales: Public Attitudes to the Use of Personal Data for Official Statistics*, 2014.

Decentralised data storage, such as the cloud, offers opportunities for holding and sharing data securely across boundaries and services. Storing data on the cloud means that rather than being held on a physical server, which may only be accessible on a certain number of devices or in certain places, data is available to anyone granted access. Tom Guthrie, former Vice President at Motorola Solutions, argues that the sector is working through ways of creating "entitlement controls", providing all employees in emergency services with unique logins to grant "person-by-person rights to information". This will have to be constructed carefully, to comply with the General Data Protection Act which will apply from May 2018.[7] Furthermore, services need to find ways of guiding responders to the relevant information, mining data to save precious time. Once in place, information-sharing could cross-cut services, allowing the individual responder to swiftly gather contextual information, such as potential security threats or mental health records, and prepare the appropriate response.

While concerns over the security of at least partly devolving data storage to third parties have been raised,[8] Neil Roberts, Chief Information Officer for Sussex and Surrey Police, argues that the big technology companies "have more IT security experts than the police have users." This echoes the majority of public-sector IT leaders, who are keen to move on-premise applications to the cloud in the near future.[9]

Emergency services could develop other technologies to further enhance security. Blockchain, a virtually un-hackable distributed ledger, is currently used in India, China and Estonia to enhance the security of medical records.[10] Blockchain networks can be private, allowing only recognised users access to sets of data, and storing a history of each time they do. This would allow organisations to hold individuals to account if they appear to access personal information irrelevant to their work.

Access at all times

Emergency services must be able to access information at all times. The Home Office is currently implementing the Emergency Services Network to replace the current TETRA network. This will transfer communications between emergency services to a commercial 4G network, enabling the transfer of data, including videos, alongside voice communications. Concerns have been voiced over the timeline and financial contingency planning for the rollout, and the National Audit Office has urged the Government to appreciate the risks of such a move, while recognising that it is the right strategic decision.[11] Before a complete roll-out, there must be absolute assurances that coverage will be at least as extensive as the current network, meaning that 97 per cent of Great Britain's landmass must have 4G coverage.[12]

Once coverage is secured, the Emergency Services Network promises to transform the frontline. With the right data sharing frameworks in place, emergency service professionals could have instant access to a world of information and guidance. It will allow services to upgrade more flexibly too, with a possible transfer to 5G in the not-to-distant future.[13] The 2015 final report of the US President's Task Force on 21st Century Policing described the access to bandwidth for emergency services as a "game-changing public safety project".[14]

7   Information Commissioner's Office, 'Overview of the General Data Protection Regulation (GDPR)', Webpage, 2018.
8   Fernando Macias and Greg Thomas, *Cloud Computing Concerns in the Public Sector* (Cisco, 2011).
9   David Bicknell, 'Public Sector CIOs Readier to Move to "as a Service" Clouds', *Government Computing*, 22 May 2017.
10   William Suberg, 'Alibaba Deploys Blockchain to Secure Health Data in Chinese First', *The Cointelegraph*, 18 August 2017.
11   House of Commons Committee of Public Accounts, *Upgrading Emergency Service Communications. Thirty-Fifth Report of Session 2016-17*, HC 770 (London: Stationery Office, 2017); The National Audit Office, *Upgrading Emergency Service Communications: The Emergency Services Network*, 2016.
12   The National Audit Office, *Upgrading Emergency Service Communications: The Emergency Services Network*.
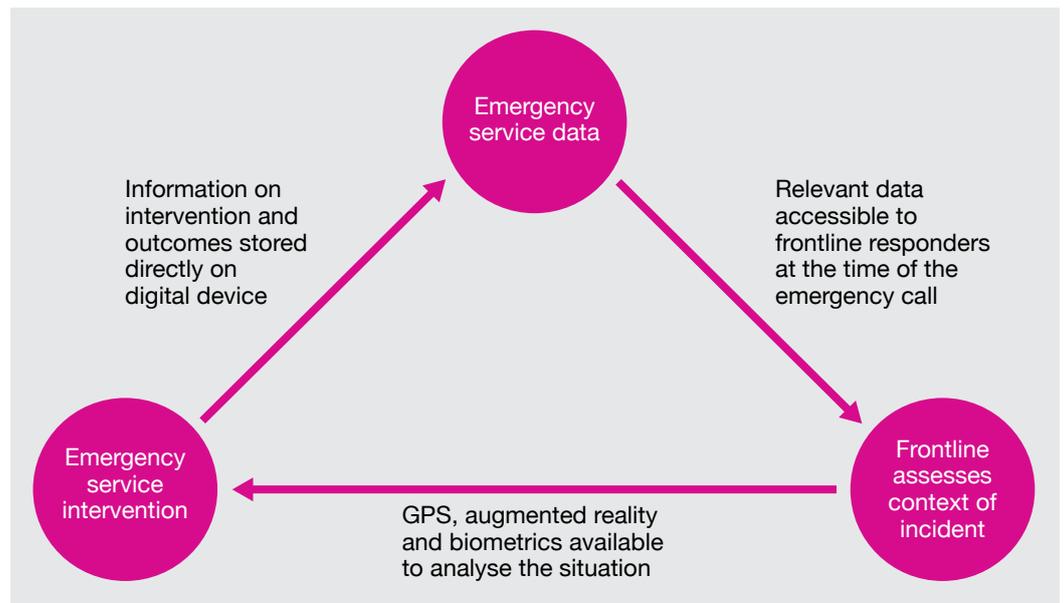13   Ibid.
14   The President's Task Force on 21st Century Policing, *Final Report*, 2015, 39.

Knowledge at emergency services' fingertips

Smart technology must then be used to get this information to police officers, ambulance crews and firefighters on the front line. Once implemented, data may flow as shown in Figure 1 below.

Figure 1: Cycle of emergency-service data

Eyes and ears: sharing information early

Technology, such as smartphones, can be used to share information with emergency services. Cartwright argues that summary information from individual patients' electronic health records should be available at the time of the emergency call, so that paramedics can plan care for a patient before the ambulance reaches them. This allows services to send the best respondent, which may not be ambulances. In London, the use of medical response cars for elderly people falling at homes reduced transfers to hospital by about 30 a week, and meant that 70 per cent of incidents could be resolved in the home.[15] The responders sent to a scene can access the digitally stored details on a mobile device on the way there, giving them a chance to prepare for the situation at hand.

On the way to an incident, responders will receive information directly from the ground. Last year, West Yorkshire Police trialled an app where users could immediately send frontline responders' multimedia messages, alerting police to the situation in advance of their arrival.[16] A police car heading to a riot could be updated by videos, text and audio recordings, all via an app on smart devices, enabling them to prepare for the emergency accordingly.

Instant data sharing can save police, fire and ambulance responders valuable time and provide the right information to help responders perform their job as effectively as possible. Drones, currently in use by the Surrey and Sussex police forces, can get to a crime scene much faster than ground security teams and quickly relay information back to frontline responders, giving them a chance to prepare the best response.[17] In San Diego, digitised lamp posts enabled by the Internet of Things, have been used to recognise gun

15 NHS Improvement, *Reducing Unnecessary Journeys and Admission to Emergency Departments for Frail Elderly People Who Fall at Home*, 2016.
16 Tom Macaulay, 'Police Trial Shows How SAS Analytics Can Improve Emergency Responses', *ComputerworldUK*, 16 February 2017.
17 Katie Jackson, 'How Drones Are Becoming Essential to Emergency Services', *Business Energy News*, 23 August 2016.

shots, and immediately alert emergency services of incidents and their precise location.[18] Gun detection tools are now sophisticated enough to help determine the direction a shooter is moving in, giving the police a greater chance of identification, and can improve understandings of public safety as much gun violence goes unreported.[19]

Situational awareness: GPS and augmented reality

Once police, ambulance or fire crews have arrived on the scene, they can use technology to aid their understanding of the situation – from recent incidents in the area to layout of buildings. Police officers in the US use applications such as 'Incident Aware', that accesses GPS data to provide information on security risks in an area, nearby officers, information on a victim's status, and enables silent requests for backup.[20] If a case develops to involve new people or a different area, officers can easily update the application to access the relevant information.

For a firefighter arriving at an incident, technology offers routes to smarter action as well. According to Alex Rhodes, the increasing use of sensors in commercial buildings may in future help to pinpoint movement and send information to a responder's mobile device, allowing them to assess how many people might be caught in a building on fire. Currently, firefighters often enter with little idea of where or how many people they should be looking for and with no reliable way for others to track their progress. Technology such as thermal imagers, which render images based on heat rather than light, can guide a firefighter safely through a building, providing real-time information on the development of the fire, and imaging through walls can monitor firefighters remotely, preventing potential life-threatening situations.[21]

Awareness of the incident upon arrival can be further improved by consulting experts based elsewhere. Police in the Netherlands are using a virtual reality command centre where augmented reality and eye-tracking technologies allow a control room operator to become completely immersed in an emergency scene.[22] The technology can be used to improve both the safety of first responders and the quality of response.

Identity management: biometrics

Although many incidents involve people already known to emergency services, some will not be identifiable upon arrival. Where there are gaps in data, emergency responders need smart and instant ways to gather information on the scene. Biometric technology can help identify these people. A 2016 Home Office report stated that the greatest opportunities in forensic analysis is to move it from laboratories to the frontline to enable analysis in "real time."[23] In February, the Home Office announced a successful trial that allowed police to record fingerprints on their mobile and identify people in under a minute.[24] With this new technology, police officers can, according to Neil Roberts, verify immediately that a suspect's name is not "Mickey Mouse", as well as speed up the process of allocating fines or discover whether a person is violating a probation. Information can then be stored on a central database to be available as court evidence if needed, cutting down on post-incident administration.[25]

Further down the line, mobile devices will have the capacity for instant facial or iris recognition, already widely used by police in the US.[26] Whether it is identifying victims of a

---

18   Hannah Griffiths, *The Future of Street Lighting: The Potential for New Service Development* (IoTUK, 2017).
19   Josh Sanburn, 'Shots Fired', *Time*, 21 September 2017; Jillian Carr and Jennifer Doleac, *The Geography, Incidence, and Underreporting of Gun Violence: New Evidence Using ShotSpotter Data* (Brookings Institution, 2016).
20   Michael Powell, 'Smartphone Cops: Apps for First Responders', *IQ intel*, 5 October 2015.
21   Airwave, *Blue Light Futures*, 2015.
22   Motorola Solutions, 'Virtual Command Centre Future Concept at PMRExpo2016', YouTube, 2016.
23   Home Office, *Forensic Science Strategy: A National Approach to Forensic Science Delivery in the Criminal Justice System*, 2016.
24   Russell Webster, 'Police Trial Mobile Fingerprinting', *Russell Webster*, 14 February 2018.
25   Airwave, *Blue Light Futures*.
26   Dave Maass, 'California Cops Are Using These Biometric Gadgets in the Field', *Electronic Frontier Foundation*, 4 November 2015.

fire or downloading the medical histories of those involved in a road accident, life-saving information could be collected through these biometric systems.

When it comes to biometric data, the need for accuracy, security and clarifications of legitimacy become acute. Tom Guthrie argues that the use of personal data and technology is a powerful tool and its uses "as variable as that of a knife." A US committee hearing earlier this year revealed that the FBI may hold facial recognition data on half of US citizens, without having conducted the necessary privacy impact assessment.[27] Furthermore, facial matching can be inaccurate, with research suggesting this is especially the case in attempts to identify black citizens.[28] Discussions about the use of biometrics, alongside other personal data, must recognise that efforts to optimise public services can carry a risk of excessive surveillance.[29] The UK Biometrics Commissioner argues that the balance between the public benefit achieved and individual privacy must be determined through Parliamentary debate and legislation, and the Data Ethics Group set up at the Alan Turing Institute should inform such debate.[30]

After the incident

The work of emergency responders does not end when an incident is over. Information needs to be logged, with significant time spent returning to a station or hospital to do so, often on slow computers. Mobile devices running on a bandwidth connection have the potential to transform this, increasing the time spent by emergency service professionals on the frontline significantly. If done correctly, it could go a long way to reduce the 27 per cent of police officer time spent on paper and computer-based administration, identified by one 2011 study.[31] The difference this makes on the frontline means, according to Neil Roberts, that for "the vast majority [of police officers], you couldn't prize it from their dead hands."

In future, responders could use mobile devices to ensure that appropriate follow-up services are accessed by users, by booking new appointments or sending them relevant information. Together with the data collected directly at the scene, this feeds into a virtuous cycle where other teams and services will be able to assess the needs of citizens quickly and accurately. It will also give responders better access to information on the outcomes for citizens, and improve their understanding of the effects of interventions.

This points to the prize of better frontline technology: more accurate information on those in need, leading to more effective responses. As technology offers evermore opportunities to improve citizens' lives, fire, ambulance and police services must be the first to seize them.

---

27   Full House Committee on Oversight and Government Reform, 'Committee to Review Law Enforcement's Policies on Facial Recognition Technology', Webpage, 22 March 2017.
28   Clare Garvie and Jonathan Frankle, 'Facial-Recognition Software Might Have a Racial Bias Problem', *The Atlantic*, 7 April 2016.
29   John Taylor, Joe Organ, and Miriam Lips, *Citizen Identification, Surveillance and the Quest for Public Service Improvement: Themes and Issues.* Paper to the European Consortium of Political Research 'Privacy and Information: Modes of Regulation' Joint Session, 2007.
30   Biometrics Commissioner, 'Metropolitan Police's Use of Facial Recognition Technology at the Notting Hill Carnival, 2017', Press release, 23 August 2017; The Alan Turing Institute, 'The Alan Turing Institute Data Ethics Group', Press release, 17 January 2017.
31   Fiona McLean, Joe Hillier, and Ipsos MORI, *An Observational Study of Response and Neighbourhood Officers* (National Policing Improvement Agency, 2011).

Bibliography

Airwave. *Blue Light Futures*, 2015.

Bicknell, David. 'Public Sector CIOs Readier to Move to "as a Service" Clouds'. *Government Computing*, 22 May 2017.

Biometrics Commissioner. 'Metropolitan Police's Use of Facial Recognition Technology at the Notting Hill Carnival, 2017'. Press release, 23 August 2017.

Carr, Jillian, and Jennifer Doleac. *The Geography, Incidence, and Underreporting of Gun Violence: New Evidence Using ShotSpotter Data*. Brookings Institution, 2016.

Centre of Excellence for Information Sharing. *Overcoming Cultural Barriers to Information Sharing within Regulatory Services*, 2016.

College of Policing. *College of Policing Analysis: Estimating Demand on the Police Service*, 2015.

Full House Committee on Oversight and Government Reform. 'Committee to Review Law Enforcement's Policies on Facial Recognition Technology', Webpage, 22 March 2017.

Garvie, Clare, and Jonathan Frankle. 'Facial-Recognition Software Might Have a Racial Bias Problem'. *The Atlantic*, 7 April 2016.

Griffiths, Hannah. *The Future of Street Lighting: The Potential for New Service Development*. IoTUK, 2017.

Health & Social Care Information Centre. *Ambulance Services, England 2014-15*, 2015.

Home Office. *Fire and Rescue Incident Statistics: England, April 2016 to March 2017*, 2017.

———. *Forensic Science Strategy: A National Approach to Forensic Science Delivery in the Criminal Justice System*, 2016.

House of Commons Committee of Public Accounts. *Upgrading Emergency Service Communications. Thirty-Fifth Report of Session 2016-17*. HC 770. London: Stationery Office, 2017.

Information Commissioner's Office. 'Overview of the General Data Protection Regulation (GDPR)', Webpage, 2018.

Jackson, Katie. 'How Drones Are Becoming Essential to Emergency Services'. *Business Energy News,* 23 August 2016.

Lewis, Brandon. 'Speech to APCC & NPCC Joint Summit on Emergency Services Collaboration', Webpage, 18 November 2016.

Maass, Dave. 'California Cops Are Using These Biometric Gadgets in the Field'. *Electronic Frontier Foundation*, 4 November 2015.

Macaulay, Tom. 'Police Trial Shows How SAS Analytics Can Improve Emergency Responses'. *ComputerworldUK*, 16 February 2017.

Macias, Fernando, and Greg Thomas. *Cloud Computing Concerns in the Public Sector*. Cisco, 2011.

McLean, Fiona, Joe Hillier, and Ipsos MORI. *An Observational Study of Response and Neighbourhood Officers*. National Policing Improvement Agency, 2011.

Motorola Solutions. 'Virtual Command Centre Future Concept at PMRExpo2016'. YouTube, 2016.

National Data Guardian for Health and Care. *Review of Data Security, Consent and Opt-Outs*, 2016.

New Statesman. *Digital Policing: The Path to 2025*. New Statesman, 2018.

NHS Improvement. *Reducing Unnecessary Journeys and Admission to Emergency Departments for Frail Elderly People Who Fall at Home*, 2016.

Office for National Statistics. *The Census and Future Provision of Population Statistics in England and Wales: Public Attitudes to the Use of Personal Data for Official Statistics*, 2014.

Powell, Michael. 'Smartphone Cops: Apps for First Responders', *IQ intel*, 5 October 2015.

Sanburn, Josh. 'Shots Fired'. *Time*, 21 September 2017.

Suberg, William. 'Alibaba Deploys Blockchain to Secure Health Data in Chinese First'. *The Cointelegraph*, 18 August 2017.

Taylor, John, Joe Organ, and Miriam Lips. *Citizen Identification, Surveillance and the Quest for Public Service Improvement: Themes and Issues.* Paper to the European Consortium of Political Research 'Privacy and Information: Modes of Regulation' Joint Session, 2007.

The Alan Turing Institute. 'The Alan Turing Institute Data Ethics Group'. Press release, 17 January 2017.

The National Audit Office. *Upgrading Emergency Service Communications: The Emergency Services Network*, 2016.

The President's Task Force on 21st Century Policing. *Final Report*, 2015.

Webster, Russell. 'Police Trial Mobile Fingerprinting'. *Russell Webster*, 14 February 2018.