Jon Mottershead, Client Executive, Atos

Digital ethics in policing

For over 200 years the UK police forces have operated to a set of nine key principles that were first articulated by Sir Robert Peel. They embody values such as building trust and co-operation with the public, preventing crime rather than just responding to it, using minimal force, and demonstrating absolute impartiality.

These principles have stood the test of time in the physical world of policing, but how well do they translate to the digital world that has brought massive changes to the way crime (now cybercrime) is viewed?

At a purely technological level, the Peelian principles arguably have some resonance with the high-level objectives of digital, particularly in the context of digital ethics. We want digital systems to build trust, to be fair, to be efficient and to prevent problems rather than cause them. But certain digital technology developments may raise barriers to implementing and enforcing such values.

When the use of data-generated insights may not be acceptable

One example is the remarkable (and sometimes alarming) insights that can be drawn from data relating to individual behaviors. Retail companies use these insights in highly personalized advertising targeting, banks use spending anomalies to help detect possible fraudulent transactions, and justice departments have even explored the possibility of assessing the probability of ex-offenders being drawn into situations where they are likely to reoffend. While most of us would probably agree that the first two examples could be acceptable use of data, there may be some serious ethical questions to ask when criminal behavior is being predicted before it has actually taken place. The mantra of “innocent until proven guilty” could be turned on its head.

Another potential scenario is where data gathered from wearable health-trackers could potentially be used as evidence that an individual was at the scene of a crime and was experiencing an elevated pulse rate at the time a crime was committed. At what point does the use of such data become an invasion of personal privacy and when is it fair to use any means possible to detect criminals? The situation is further complicated by the use of CCTV facial recognition, as it indiscriminately applies invasive analytics to all. This is already seen by some as a potential restriction to freedom of movement.

We may be astounded by the feats of analytics and AI algorithms to identify crime hot spots or to predict when and where criminal activity is likely to occur, but we have to remember that the “bad guys” have access to the same kind of technology and might use it to work out how to best avoid police presence. In addition, cybercrime has little respect for physical geographical borders: to ensure protection against global threats, the Peelian principle of building trust and co-operation with police forces round the world has to be reimagined.

At what point does the use of such data become an invasion of personal privacy and when is it fair to use any means possible to detect criminals?