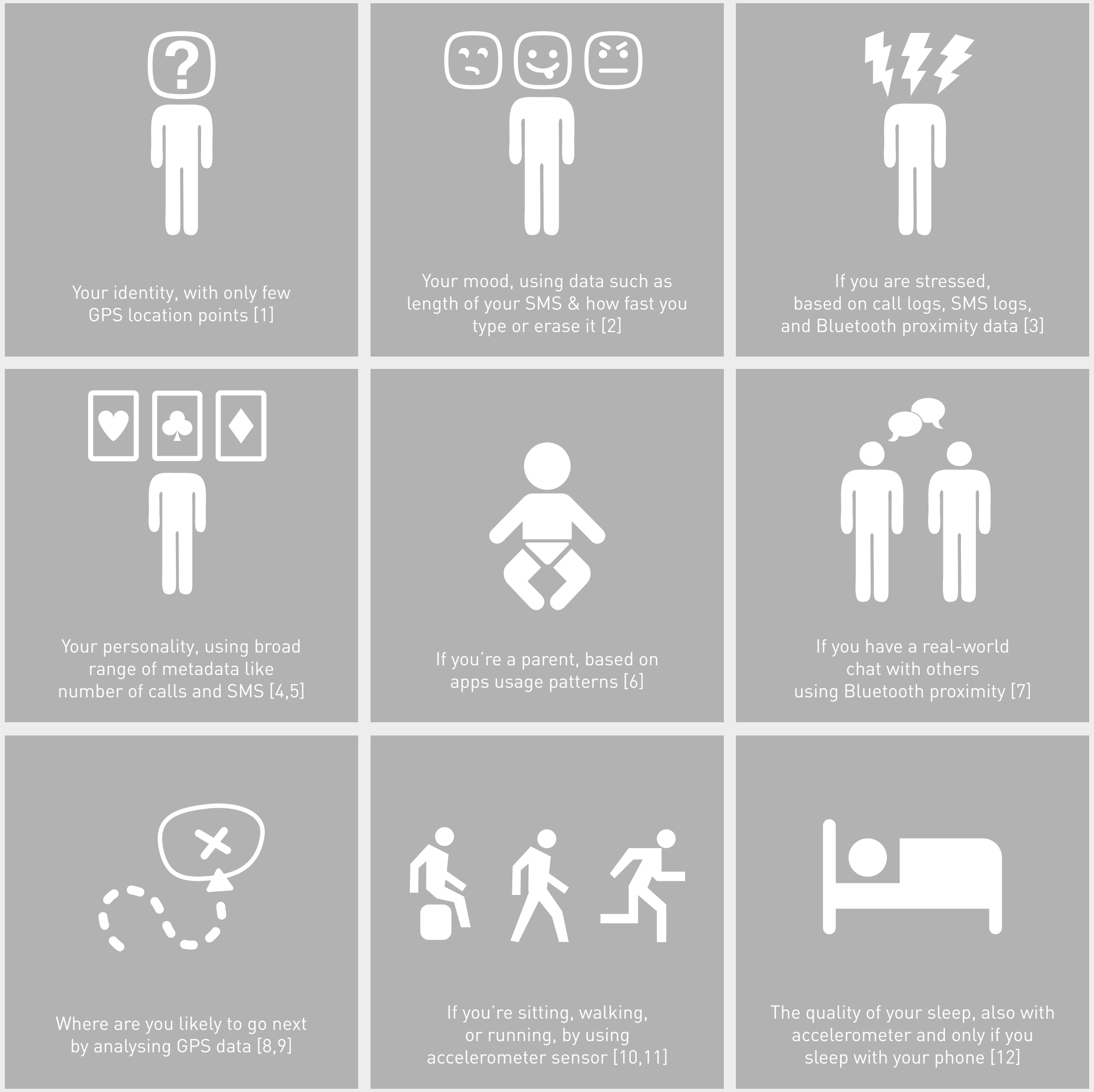
WHAT YOUR PHONE SAYS ABOUT YOU?

LUKASZ PIWEK & ADAM JOINSON | UNIVERSITY OF BATH



Your identity, with only few GPS location points [1]

Your mood, using data such as length of your SMS & how fast you type or erase it [2]

If you are stressed, based on call logs, SMS logs, and Bluetooth proximity data [3]

Your personality, using broad range of metadata like number of calls and SMS [4,5]

If you're a parent, based on apps usage patterns [6]

If you have a real-world chat with others using Bluetooth proximity [7]

Where are you likely to go next by analysing GPS data [8,9]

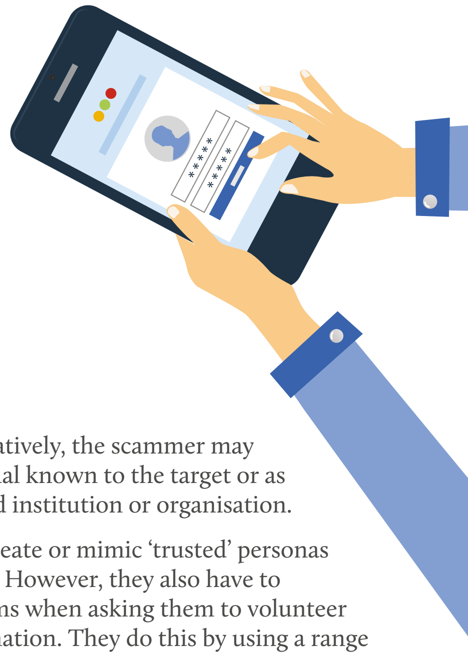
If you're sitting, walking, or running, by using accelerometer sensor [10,11]

The quality of your sleep, also with accelerometer and only if you sleep with your phone [12]

[1] de Montjoye, Y.A., et al. (2013). *Scientific reports*, 3, 1376; [2] Lee & Park(2012). *Proceedings of IEEE CCNC*, 260–264; [3] Bogomolov, A., et al. (2014). *Proceedings of the ACM*, 477–486; [4] Chittaranjan, G., et al. (2013). *Personal and Ubiquitous Computing*, 17, 433–450; [5] de Montjoye, et al. (2013b). *Behavioral-Cultural Modeling and Prediction*, 48–55; [6] Seneviratne, S., et al. (2014). *ACM SIGMOBILE Mobile Computing and Communications Review*, 18, 1–8; [7] Osmani, V., et al. (2014). *Journal of Ambient Intelligence and Humanized Computing*, 5, 297–306; [8] Song, C., et al. (2010). *Science*, 327, 1018– 1021; [9] Do, T.M.T. & Gatica-Perez, D. (2014). *Pervasive and Mobile Computing*, 12, 79–91; [10] Wu, W., et al (2012). *Journal of Medical Internet Research*, 14, e130; [11] He, Y. & Li, Y. (2013). *International Journal of Distributed Sensor Networks*, 2013, 1–10; [12] Natale, V., et al. (2012). *Sleep and Biological Rhythms*, 10, 287–292.

EMMA WILLIAMS AND ADAM JOINSON

Eliciting Information Online



In November 2015, the Metropolitan Police Service reported that they had investigated £4m lost through internet dating scams in the previous 12 months. Given the likely under-reporting of losses by victims, it is probable that this figure represents a small portion of the total amount lost by UK internet users. In fact, in 2012 it was suggested that almost a quarter of a million people in the UK may have fallen for an online dating scam, a figure likely to have increased given the growth in online dating during the last four years. Online dating and romance scams work in part because relationships formed over the internet are vulnerable to 'hyperpersonal' patterns of interaction characterised by intense, accelerated feelings of closeness, rapport and trust. Because of this, the internet often provides an ideal environment for those with malevolent intent to elicit information from victims (see Box).

The nature of online communication means that scammers are able to strategically present and edit information about themselves, presenting profiles that appear similar (through apparent shared common interests or group membership) or attractive to the victim. For instance, online romance scams mimic coveted gender stereotypes in their profiles, such as wealthy widowers, military personnel, and young females in caring roles like nursing. Fake social media profiles have been used to infiltrate online networks of military and defence personnel, with such attempts being successful despite the presence of inconsistencies in profile information. Alternatively, the scammer may pose as an existing individual known to the target or as a representative of a trusted institution or organisation.

Online scams attempt to create or mimic 'trusted' personas in order to appear genuine. However, they also have to address the doubts of victims when asking them to volunteer potentially sensitive information. They do this by using a range of influence techniques that attempt to limit how deeply an individual processes information, encouraging them to make relatively automatic decisions based on stereotypes and biases.

This includes creating scenarios that invoke a sense of urgency so that victims feel they don't have sufficient time to verify them, or creating an imminent crisis and asking for help so that people feel obliged to respond, particularly if emotions such as empathy, guilt or anxiety are invoked. For this to work they have to generate an emotional response from the victim through helping them identify with the character and situation they are presenting. Techniques designed to create an obligation of reciprocity in the future may also be used, such as providing free gifts or favours and requesting information in return. This combination of 'editable' online personas and complex influence scenarios may make people particularly vulnerable to information elicitation attempts in online environments.

Causes of hyperpersonal interaction

There are a number of reasons why people often form overly positive, trusting relationships online that make elicitation of information more likely. These include:

Selective self-presentation: people choose what to communicate about themselves online – and usually that will be more positive aspects of themselves.

Idealised impressions: the person on the receiving end of these positive self-presentations often forms an idealised impression, with fantasy and social projection filling in the gaps.

Confirmation biases: Once we form a positive impression of someone, we often seek information to confirm the initial positive impression, leading to a feedback cycle of positive impressions and increased liking.

Uncertainty reduction: People tend to disclose more information about themselves online – one reason being that uncertainty makes us uncomfortable. We tackle this uncertainty by asking more probing questions. We also tend to disclose more information about ourselves, which encourages the other person to reciprocate.

Emma Williams and Adam Joinson research scamming techniques and are based at the University of Bath.