Security and Privacy in a Digital Age: A Response to M34 (2013)

1. At the Methodist Conference of 2013, the following memorial was presented:

    1.1. **M34 Personal tracking software**: Having noted press reports about the tracking of personal information from social networking sites using Raytheon's Riot (Rapid Information Overlay Technology) software, the Liverpool District Synod (R) (Present: 85; Voting: 76 for, 0 against) requests that the Conference explore with ecumenical partners raising with our government our concerns over the control and possible abuse of Riot as a threat to personal freedom and privacy.

2. The following reply to the Memorial was agreed by the Conference:

    2.1. The Conference thanks the Liverpool Synod for its memorial. The memorial raises difficult questions about what is public and what is private, and the rights over what lies in between. The recent disclosures about the use of PRISM, covered widely in the international press, and which implicated social media platforms and governments alike, make the issues outlined in the memorial even more pressing.

    2.2. The growth of social media, internet transactions and the use of mobile technologies means that there are massive amounts of data available which can help build up a detailed picture of a person's behaviours, locations, activities and preferences. There are concerns, such as those expressed in this memorial, that such data may be used by government or private companies to infringe the privacy of individuals.

    2.3. It is important for individuals to recognise that once they have an online presence, they will create a significant amount of data about themselves. Some of this can be restricted by an active use of privacy settings; much of it is hard to avoid.

    2.4. Many people will feel uncomfortable about having personal data freely available, and particularly if such data may be mined and exploited by commercial organisations. While the use of such data does fall under the Data Protection Act and other legislation, it is clear that in the age of Big Data and while the government remains uncertain about whether to create new legislation covering this issue, the situation is extremely complex.

    2.5. It is clear that the Connexional Team would need to develop a wide body of knowledge and experience to respond directly to this memorial, necessarily entailing a disproportionate use of time and resources, which should be used to greater effect on other issues. However, the Conference notes that there are good Methodist links with the CODEC research team at St John's College, Durham University. CODEC's remit is to explore Christianity within the digital age and issues related to theology in the digital age. The Conference therefore directs the Methodist Council to address the concerns raised in the memorial by inviting CODEC to work with the Connexional Team to produce a report, drawing on academic, ecumenical, governmental

and digital industry links, to provide further guidance for the Church on these matters.

Background

3. In compiling this response, CODEC drew upon:

   3.1. Press reports and editorial comment on the NSA/PRISM crisis, especially the huge repository offered by the Guardian newspaper[1]

   3.2. Seminars either attended at digital culture conferences or offered through the web given by leading experts in the field[2]

   3.3. Government briefings on the various acts being processed by the UK and EC governments on security, digital inclusion, and digital governance processes[3]

   3.4. OfCom and Oxford Institute of Internet Studies Briefings and Reports[4]

   3.5. Additional alternative views[5]

4. The very fact that we choose to go online makes us vulnerable. Indeed, every engagement with the digital world potentially gives technology firms and data collection farms the chance to track our every move and every keystroke. Mobile phones track our GPS co-ordinates, or log which signal beacon we are connected to, or harvest our phone calls, our pictures and our texts into their cloud repositories. Twitter and Facebook encourage us to share whom we know, our travel arrangements, our social activities, everything. Google collates our buying history and fills our webpages with the adverts it thinks we might be most tempted by. We are told so often that these companies are acting for our

---

[1] http://www.theguardian.com/world/the-nsa-files

[2] Thinking Digital 2011-2013; talks by Harvard's Professor Bruce Shneier (http://www.ted.com/talks/bruce_schneier); talks by Mikko Hyponnen (http://www.ted.com/talks/mikko_hypponen_how_the_nsa_betrayed_the_world_s_trust_time_to_act); talks by Alessandro Acquisti (http://www.ted.com/talks/alessandro_acquisti_why_privacy_matters); Newsnight interview with Glenn Greenwald (https://www.youtube.com/watch?v=f1Zvo8N3G94); Blogposts by Lucian Hudson, Open University (http://open.ac.uk/blogs/lucian-hudson/)

[3] Government Service Design Manual on Information Security (https://www.gov.uk/service-manual/making-software/information-security.html); HMRC briefing on online security (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/89027/online-security.pdf); Parliamentary Briefing on Cyber Security in the UK (http://www.parliament.uk/briefing-papers/post-pn-389.pdf); Patrick Dunleavy and Helen Magretts, "The second wave of digital era governance" (http://eprints.lse.ac.uk/27684/1/The_second_wave_of_digital_era_governance_(LSERO).pdf)

[4] Ofcom Communications Market Reports (with analysis) 2004-2013 (http://stakeholders.ofcom.org.uk/market-data-research/market-data/communications-market-reports/); Oxford Internet Surveys (http://oxis.oii.ox.ac.uk)

[5] Electronic Frontier Foundation (https://www.eff.org/nsa-spying); see also the two novels by Cory Doctorow: *Little Brother* and *Homeland* (available from bookshops or free from http://craphound.com); "Calm Down Dears" debate on *IntelligenceSquared.com* (http://www.intelligencesquared.com/events/state-snooping-is-a-price-worth-paying-for-security/)

benefit – to provide us with the services we never knew we needed. And now, since Snowden's grand whistleblowing about PRISM and the NSA, we find that not only is our security and privacy compromised for commercial reasons, but also our emails, tweets, and updates, even our mobile calls and texts, can be scanned through data surveillance, carried out by both UK and USA security agencies, just to check who the real terrorists after all![6]

5. Simply being online means your personal data could be compromised. However, extricating ourselves from digital culture is increasingly hard in a 'digital by default' and 'surveillance-addicted' society. Stepping outside of your door is quite likely to expose you to a plethora of CCTV cameras, the modern equivalent of the twitching net curtain – in public spaces, supermarkets, shopping malls, hospitals, hotels, banks, restaurants, pubs. Wherever you go, it is likely that you will be seen and your actions logged by a data-recorder somewhere.

6. For example: the Metropolitan police were recently given access to all the cameras which form the perimeter of the Congestion Zone in London, alongside *Transport For London* cameras and other surveillance cameras already in place (bus lane cameras, etc). This network of surveillance cameras mean that when allied to numberplate recognition technology (NPR), even the most innocent journey across London is probably being logged and stored in a data centre somewhere. But this 'invasion of privacy' has already led to crimes being solved – including a rape case where a woman was kidnapped in a car in Kensingston and eventually released in East London in the early hours of a Saturday morning. The police were able to track which cars had made that kind of journey that evening, and eventually found the car, traced the driver and arrested the rapist. In that instance, data surveillance becomes a boon to the common good. We want surveillance because it protects us.

7. Facial recognition technology is the next step in surveillance camera technology. Why not scan every face that comes into an office block/student accommodation and be able to link that face to a person who has the right to be there? That provides protection for vulnerable people. It also logs exactly who has attempted entry into any space. It also needs a massive identity database to enable the face recognition which could lead to a massive biological database recording the identity of everyone with a right to be anywhere in the UK.

8. Digital disengagement is no longer an option. Access to information, and applications for benefits, registrations, fines, taxes, and perhaps even to voting will soon be wholly digital. Lack of an ability to engage with the digital already leads to training programmes. In today's society, the digital inept are becoming a socially unacceptable class since they hold back Digital Britain in its race to the front of the Digital Queue. But as we move into more and digital health provision and monitoring, a Digital Britain will mean that access to the very basic elements of civic society will demand digital engagement - health, shopping, government services, banking, the right to free movement.

[6] The Guardian have compiled an excellent video about all this in their Made Simple series: https://www.youtube.com/watch?v=GoM4jlZbTtQ

9. However, we must remember that the vast majority of stored personal and public data is rarely analysed by a human being and even then usually anonymised. The databases which the NSA, GCHQ and Google create from data farming offer a corpus of material which computers sift via 'distant reading' to distil peculiar patterns and unexpected data. The results of 'distant reading' will then be promoted to more forensic analysis by more powerful search programmes long before being given to an actual human being to explore through 'close reading'. These are the normal processes used in digital humanities and in *Corpus Linguistics*. So, at the *Thinking Digital Conference* in 2012, Boeing's head of data security outlined similar processes his own company used on the US government's behalf to alert data analysts of irregularities that might signal a security alert.

10. As such, the key fact to remember is that your data, your church's data, and the Church's data is unlikely to represent a level of abnormality which would be of interest even in a "surveillance-addicted" society. If we lived in a police state where religion was prohibited, then the algorithms would highlight the Church and its officers and members as targets. But we don't.

11. However, surveillance has its uses. We must remember that if we want to remove child pornography from the web, then the kind of machine-based distant reading of every search request and every piece of digital communication for certain offending text-strings and digital practices is absolutely necessary. Such protection demands surveillance and a removal of surveillance would lead to the dystopia of the DarkNet.

12. Moreover, so much data being collected by government, business, and the Third Sector that much of it has to be completely ignored unless it can be found to have a commercial use. Data is only valuable when it is a tradeable commodity. As such, Google is much more interested in your online purchasing than in your religious activity online. Emails to and from Church Council members are sometimes confidential but rarely of commercial interest. Although, as we all know, sensitive data has to be treated sensitively

13. The Church will want to argue properly against commercial exploitation of private data, invasion of privacy, and the breaking of confidentiality. It is likely that the potential for such exploitation will develop further as digital culture becomes even more embedded within contemporary societies across the world. It may well be that a future report is needed which explores how the Church might properly and reasonably argue its case within the wider debates on human rights and responsibilities.

14. The Church will also want to encourage its members to be aware of the need to engage in digital culture carefully and with sensitivity. The Methodist Church's *Social Media Guidelines* might be extended to offer a *Digital Health Check*, or even a digital culture version of Sangster's *A Spiritual Check-up* – a way of encouraging discipleship in the digital age – and of promoting digital good practice such as issues of distraction, omnipresence, 24/7 contactability, confidentiality, anonymity, social sharing, blogging for public figures, digital

sabbaticals, even details such as an awareness of the impact of screens on neural sensitivity at night.

15. There must be limits to surveillance in order to provide some protection concerning individual and personal rights? Bruce Sneier, leading data security academic at Harvard University, has explored the right of privacy around medical data and other data relating to an individual's rights to privacy. Sneier's work shows how the fight for privacy is not always about attempts to hide criminal/sinful/salacious activity. Privacy is also about maintaining boundaries around private information about ourselves which we choose not to place in the public domain.

16. Within the Methodist Church, we have already discussed confidentiality as part of professional practice in the report adopted by the Conference in 2008, *With Integrity and Skill*, and in the subsequent guidelines on confidentiality available online (http://www.methodist.org.uk/downloads/conf08_confidentialityguidelines_0808.pdf). These guidelines, along with the Methodist Church's social media guidelines (http://www.methodist.org.uk/ministers-and-office-holders/technology-and-church/social-media-guidelines) make it clear that all of our communication with others needs to be treated sensitively. We always need to consider the level of privacy assigned to or assumed in each piece of communication. What you write/type/text/say depends on who is listening/receiving/reading. The Church's internal and external communication will often involve elements of confidentiality and inter-personal relations which need careful management and control in order to protect the right to privacy and confidentiality to individuals involved.

17. So, for example, coming home from a difficult meeting and sending out a Facebook message suggesting that the Church Council are incompetent not only has an negative effect on those who read it (and probably even more from those who hear about it over coffee on the next Sunday), but also brings the actions of that entity and its constituents into question in an unhelpful way. What we put online, even in private communication, is subject to the normal laws governing publication in the UK – including libel and defamation. Letting off steam on the 'net at the expense of other people's privacy is not acceptable practice, either in the Church or in the rest of society.

18. Complete privacy is impossible in the contemporary digital world. Indeed, there is good Biblical evidence to suggest that complete privacy is something to avoid. Although, in the Sermon on the Mount, we are encouraged to keep some activity, such as charitable giving, to ourselves, we are also told to keep ourselves in the light, in the open, like a city on a hill. We, who are called to live as witnesses to the transforming power of God, will want to ensure all our communications and all our dealing with the personal data and confidentiality accords with that callings. We will want to avoid acting as though we have something (digital) to hide. But at the same time, we will want to protect the rights of confidentiality and personal/corporate identity which are essential to human flourishing. The

need is there to maintain the right balance – allowing appropriate surveillance for the common good, while maintaining the definition of personal boundaries necessary in any complex society.

19. Therefore protecting privacy is not just an issue done for us. Protecting privacy and protecting other people's rights to privacy is an issue we need to make part of our own digital agenda. Security and vigilance is needed at all times.

20. Recommendations

20.1. The Methodist Council encourages this report to be discussed in Church Councils and staff meetings and for appropriate conversations to be held and outcomes to be fed back to the Communications Team at Methodist Church House.

20.2. Alongside all those employed by the Methodist Church, all members and ministers of the Methodist Church are encouraged to adhere to the Social Media Guidelines of the Methodist Church and the Guidelines on Confidentiality.

20.3. Steps should be taken in every circumstance to protect and secure data stored by the Church through proper security of computer hardware (secure office environment where computers can only be accessed by the proper people) and also proper use of security protocols on that hardware (passwords, automatic secured screensavers to protect computers left unattended, up to date virus checkers, possibly even avoidance of cloud-based data services)

20.4. The Methodist Council directs that the Methodist Church's *Social Media Guidelines* be extended to offer a *Digital Health Check* which should be made available online and promoted for use across the Connexion and beyond

20.5. The Methodist Council directs JPIT and the Communications Team to consider whether there are appropriate ways to work with ecumenical partners in highlighting the problem of commercial exploitation of private data

Appendix A

Approaches to personal privacy

Here are three examples of steps internet gurus or journalists have suggested of ensuring great security for your digital engagement. But are all the following too scary and too technical? Some of them offer some bad advice compared to Methodism's own Social Media Guidelines – especially the last one from the Guardian, which deserves a workshop on its own!

Steven Vaughan Nichols

(http://www.zdnet.com/six-ways-to-protect-yourself-from-the-nsa-and-other-eavesdroppers-7000016860/)

1. Abandon the cloud – or don't go there in the first place…
2. Stop texting and using most instant messaging services
3. Encrypt your e-mail
4. Hide your Web browsing
5. Turn off all services you don't need
6. Quit social networks: all of them!

Brian Fung

(http://www.smh.com.au/digital-life/digital-life-news/six-ways-to-guard-your-privacy-online-20130906-2t9f2.html#ixzz2qSz780yY)

1. Encrypt your email
2. Encrypt your chats
3. Enable incognito mode on your web broswer
4. Use a traffic anonymising service such as Tor
5. Pay for a private VPN
6. Use a password manager

Jon Lawrence and Sean Rintel
(http://www.theguardian.com/commentisfree/2013/dec/03/eight-ways-to-protect-your-privacy-online)

1. Use a password manager
2. Disable GPS and Wi-Fi on your mobile device until you need them
3. Read the access privileges for apps carefully, and make good choices
4. Guard your date of birth and telephone number
5. Make yourself more difficult to find on social media
6. Keep your work and personal presences separate
7. Encrypt your connections
8. Collective action