# SCOTTISH SOVEREIGNTY IN THE AGE OF MASS SURVEILLANCE

## THE CASE FOR OPEN SOURCE PROCUREMENT

**Alistair Davidson**
Open Rights Group Scotland Advisory Board

Research: Tia MacFarlane

COMMON WEAL POLICY

# Executive Summary

The Daily Record revealed on 24 July that guidelines which prevented UK secret service agencies spying on devolved governments, known as the Wilson Doctrine, had been scrapped, leaving the correspondence of politicians in the Scottish Parliament, as well as the Welsh and Northern Irish Assembly, open to being hacked.

This has placed urgent emphasis on finding a new solution to ensure Scottish data sovereignty. Even if the Wilson Doctrine was restored it would offer little protection, as it is not enforceable in law.

This paper looks at the implications of whistle-blower Edward Snowden's revelations of the global nature of US and UK mass surveillance of innocent citizens and businesses. It looks at the case of spying on the Brazilian national oil company, Petrobas, and the response of the Brazilian government. It makes the case for the adoption by businesses and government of publicly auditable open source software to protect Scottish sovereignty, and argues that Scotland could quickly become a global leader in an emerging market for open source software.

The key recommendations of the paper are as follows:

1. **A national open source transition plan** with urgent attention given to infrastructure critical to national security.

2. **Amend government procurement legislation to favour open source software**, recognising that software code that is publicly auditable is more trustworthy and publishing code under open source licenses has substantial community benefit.

3. **Pay for the open source licensing of existing software**. Public sector bodies should, wherever possible, negotiate for existing third-party software to be relicensed as open source.

4. **Amend Scottish Enterprise guidelines to better support open source software**, including the commercialisation of open source and the development of innovative new user interfaces.

5. **Recognise and invest in critical infrastructure** by establishing a stream of grant funding for projects deemed critical to Scottish security, sovereignty and commerce.

6. All Scottish Government communications should be sent over encrypted channels, **and encryption strongly encouraged in the private sector.**

# 1. Introduction

This paper will seek to address the implications of Edward Snowden's revelations for Scottish sovereignty. It will review the evidence that surveillance programmes of the United States of America and the United Kingdom have been used to invasively monitor the innocent citizens and businesses of foreign sovereign states. It will examine the case that the National Security Agency (NSA) targeted the Brazilian national oil company, PetroBras. Finally, it will set out the case for the widespread adoption of publicly auditable open source software by Scottish businesses and government in order to protect Scottish sovereignty, and recommend actions that the Scottish Government can use to promote open source software.

The Scottish parliament is gaining increased powers and responsibilities at a time when use and regulation of the internet is in flux. This period of rapid change creates new threats and offers new opportunities. In order to assert and protect its sovereignty, Scotland must develop a bold and assertive approach to communications technology. While the Scottish Government does not control levers such as taxation, through its procurement budget and Scottish Enterprise grants it has substantial powers to create, grow and mould software markets.

This has been made especially urgent by revelations in the Daily Record that "the UK's electronic eavesdropping agency last month dumped guidelines which had constrained spies from tapping MSPs' phones or hacking their emails."[1] Even if the Wilson Doctrine against spying on elected politicians was restored for devolved administrations, it would offer scant protection, as it "does not have force in law and cannot impose legal restraints on the agencies,"[2] and does not protect businesses or private citizens.

The Claim of Right, originally written in 1989 and passed by the Scottish Parliament[3] in 2014, asserts the sovereign right of the Scottish people to choose their government. Implicitly, this government must exercise sovereign power over the territory and resources of Scotland. This requires that no other state can intervene in Scottish internal affairs, particularly as regards its "political independence or territorial integrity"[4].

It is unlikely that Scotland will be subject to major breaches of physical sovereignty[5], for example, foreign troops occupying a Scottish oil platform. There is however a significant danger that the intelligence services of foreign governments could affect, for example, the sale of the rights to a Scottish oil field. It is certain, in the short term, that they will surveil the government, businesses, and indeed the entire population of Scotland. Defence against this must be included in our understanding of what it means to be sovereign in the 21st century.

The security services of the Five Eyes intelligence alliance countries - the USA, UK, Canada, Australia, and New Zealand - have developed a global system of total surveillance unprecedented in human history. This system collects and stores as much internet traffic as it can, and provides it in searchable format to as many as 850,000 intelligence analysts and contractors in the USA alone. It records, to the limits of affordability, the entire online lives of every citizen of Scotland.

German Chancellor Angela Merkel went so far as to compare this system to the STASI[6]. In fact whereas the STASI held its files on East German citizens in 48,000 filing cabinets in Berlin, if the NSA were to print the data it stores on the world's citizens, it would require 42,000,000,000,000[7] filing cabinets, which would overflow the entire territory of the European Union.

1 www.dailyrecord.co.uk/news/scottish-news/snoopgate-scandal-brit-spooks-spying-6127095

2 www.theguardian.com/uk-news/2015/jul/24/wilson-doctrine-unworkable-bulk-interception-intelligence-agencie

3 www.scottish.parliament.uk/S4_BusinessTeam/pm-v1n48-S4.pdf

4 www.un-documents.net/a25r2625.htm

5 www.reidfoundation.org/wp-content/uploads/2012/10/No-Need-to-be-Afraid2.jpg

6 www.theguardian.com/world/2013/dec/17/merkel-compares-nsa-stasi-obama

7 apps.opendatacity.de/stasi-vs-nsa/english.html

The surveillance system undermines the internet security on which all modern commerce depends. It has made the internet more vulnerable to attacks by state and non-state actors alike. It has also allowed the NSA to attack foreign businesses, including PetroBras, the Brazilian national oil company. The NSA has of course denied that it engages in commercial espionage[8], but it is unclear what other purpose this surveillance could have served.

It is important to consider that in the event of Scottish independence or Home Rule, the remaining United Kingdom (rUK)'s intelligence services would still be a part of this surveillance system. While an independent Scotland might be offered the chance to become a sixth member, it is highly unlikely that this relationship could ever be symmetric. An independent Scotland that took this path would surrender control of its commerce and total knowledge of its people to foreign powers. Its new-found sovereignty would be in name only.

To protect its sovereignty, any modern state must be able to secure its internet traffic. The routing and processing of internet traffic is handled by computer software. The behaviour of this software is crucial to computer security. All software is written in an English-like language, which is called the software programme's source code. This is transformed into a machine readable language before the software is run.

A key enabler of the NSA's actions has been the widespread use of software that is ordinarily distributed solely as machine code, and whose behaviour cannot be modified by end users. This is called proprietary software. The effect is that the purchaser cannot be certain of how the proprietary software behaves. It cannot be audited and corrected by the global computer security community, giving the NSA privileged access to security vulnerabilities, and even, in certain cases, the opportunity to implant deliberate vulnerabilities.

This stands in contrast to open source software, which runs the majority of the world's internet servers[9] and can be found at the core of all Android phones. Open source software makes available both its machine and source code. Equally importantly, open source copyright licenses allow the software to be modified and redistributed. This allows businesses, governments, and independent researchers to collaborate on auditing and improving the software. Early fears that removing restrictions on redistribution would prevent the development of profitable businesses have proven unfounded[10]. The largest producer of open source software, Red Hat Inc, has a market capitalisation of $9.5bn[11].

The Brazilian and Chinese governments are both turning to open source software to protect their sovereignty. China has gone so far as to ban Windows 8 on government computers[12]. This represents a tremendous opportunity for any company or country willing to seize it. Bold policies by the Scottish government could create a global centre for open source development.

8 www.bloomberg.com/news/2014-01-24/nsa-surveillance-rules-will-keep-ban-on-commercial-spying.html

9 secure1.securityspace.com/s_survey/data/201403/index.html

10 www.recode.net/2014/03/25/a-perfect-storm-moment-for-multibillion-dollar-open-source-companies/

11 finance.yahoo.com/q/ks?s=rht

12 www.bbc.co.uk/news/technology-27712908

# 2. Challenges for Scotland

### 2.1 The Scope of Surveillance

According to Edward Snowden's leaks, NSA, GCHQ, and allied surveillance sweeps up a large part of internet traffic. He testified to the European Parliament that "The NSA granted me the authority to monitor communications worldwide using its mass surveillance systems, including within the United States. I have personally targeted individuals using these systems … and I am telling you that without getting out of my chair, I could have read the private communications of any member of this committee, as well as any ordinary citizen."[13]

#### 2.1.1 PRISM

PRISM is a joint NSA and GCHQ programme that gathers data directly from nine participating internet companies - Microsoft, Yahoo, Google, Facebook, PalTalk, YouTube, Skype, AOL, Apple, allowing even low-level intelligence analysts to access "whatever emails they want, whatever telephone calls, browsing histories, Microsoft Word documents."[14]

#### 2.1.2 Tempora

Tempora is a GCHQ programme that directly taps 200 international fibre-optic cables, with the knowledge of either the owner of the cable or the landing station. Data collected includes all telephone calls and emails passing through the cables. 850,000 NSA employees and US private contractors have access to this data, in addition to GCHQ analysts[15].

#### 2.1.3 Muscular

Muscular is the best-evidenced example of joint NSA and GCHQ programmes that target traffic internal to major internet companies, including Yahoo and Google, without the knowledge of those companies. This included copying entire email accounts at a time[16]. Google, Yahoo and other internet companies have since taken steps to encrypt their internal traffic[17].

#### 2.1.4 Xkeyscore

XKeyscore is NSA analysis software, shared with other agencies, that analyses the data collected by surveillance programmes. Edward Snowden claims that as a low-level analyst or contractor, "You could read anyone's email in the world, anybody you've got an email address for. Any website: You can watch traffic to and from it. Any computer that an individual sits at: You can watch it. Any laptop that you're tracking: you can follow it as it moves from place to place throughout the world."[18]

### 2.2 Proprietary Software and the NSA

The NSA has exploited the unauditable nature of proprietary software to insert backdoors, deliberate security defects ostensibly known only to the NSA. It is not known if any other intelligence services, criminals, or other actors have successfully used NSA backdoors. It has been confirmed that the NSA receives advance notice of vulnerabilities and does not report those that it discovers itself, allegedly including the recent Heartbleed bug that affected two thirds of the world's web servers[19].

There are several well-evidenced cases of the insertion of backdoors and other attacks on internet security by the NSA.

13 www.europarl.europa.eu/document/activities/cont/201403/20140307ATT80674/20140307ATT80674EN.pdf

14 www.abcnews.go.com/blogs/politics/2013/07/glenn-greenwald-low-level-nsa-analysts-have-powerful-and-invasive-search-tool/

15 www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

16 apps.washingtonpost.com/g/page/world/how-the-nsas-muscular-program-collects-too-much-data-from-yahoo-and-google/543/#document/p3/a129339

17 www.washingtonpost.com/business/technology/google-encrypts-data-amid-backlash-against-nsa-spying/2013/09/06/9acc3c20-1722-11e3-a2ec-b47e45e6f8ef_story.html

18 www.ndr.de/ratgeber/netzwelt/snowden277_page-3.html

19 www.bloomberg.com/news/2014-04-11/nsa-said-to-have-used-heartbleed-bug-exposing-consumers.html

As long ago as 1997, IBM admitted that their Lotus Notes email software contained an NSA backdoor as a condition of export[20]. At the time, Lotus Notes was the biggest-selling email software in Europe, used by many governments and strategically important businesses. American export restrictions classified strong encryption as a weapon, and required IBM to weaken security for export markets. The Lotus Notes export license was conditional on the NSA having a privileged ability to access the emails of foreign citizens, governments and businesses.

In 2004, the leading security company RSA took payment of $10m[21] from the NSA to use the Dual_EC_DRBG algorithm as standard in its products. Security researchers identified this algorithm as probably containing an NSA back-door in 2007[22], but its use by RSA continued until 2013, when Edward Snowden's revelations proved beyond doubt that the backdoor was real.

In the wake of Snowden's revelations, Microsoft admitted that it "provides intelligence agencies with information about bugs in its popular software before it publicly releases a fix"[23]. Microsoft's software is present on over three quarters of desktop and laptop computers[24]. This renders Microsoft's Government Security Programme, which offers private but not public auditability[25], effectively worthless - a private audit might find a deliberate backdoor, but it could never hope to identify all vulnerabilities.

Taken together, these practises leave internet users, the Scottish Government, and businesses open to attack not only by the NSA and allied intelligence services, but by other intelligence services such as those of the Chinese and Russian governments, criminal organisations, terrorists, and other non-state actors. They are a threat to the integrity of the internet itself, and a threat to all trade conducted there.

53 American security and cryptography experts issued an open letter accusing the NSA of "fundamentally undermining the security that enables commerce, entertainment [and] personal communication."[26]

None of these attacks were detected, except where admitted or leaked, because this software cannot be audited by the global security community. Until now, businesses and governments outside of America have trusted the American software industry to create secure products, and have not audited those products. It has become clear that the proprietary software model cannot provide a secure and trusted internet infrastructure.

### 2.3 The Petrobras Case

In September 2013, leaked slides revealed that as part of the NSA's Black Pearl surveillance programme "private network traffic is collected from energy companies, financial organisations and airlines, as well as foreign governments"[27]. In particular, Brazil's national oil company PetroBras was targeted at a time when it was involved in the auction of rights to exploit some of the largest oil fields in the world[28]. Brazil's President Dilma Rousseff described the NSA's actions as "tantamount to industrial espionage" with "no security justification"[29].

While there is no direct evidence that this surveillance affected the sale of any oil rights, the possibility cannot be ruled out. The PetroBras case makes absolutely clear that without protection of strategic computer systems, a nation cannot expect to retain sovereign control of its natural resources. As we saw in Section 2.2, the required level of security is not possible while using proprietary software.

20 catless.ncl.ac.uk/Risks/19.52.html#subj1
21 www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220
22 www.schneier.com/blog/archives/2007/11/the_strange_sto.html
23 www.bloomberg.com/news/2013-06-14/u-s-agencies-said-to-swap-data-with-thousands-of-firms.html
24 www.netmarketshare.com/operating-system-market-share.aspx
25 news.cnet.com/Governments-to-see-Windows-code/2100-1006_3-980666.html
26 http://masssurveillance.info/
27 http://www.theguardian.com/world/2013/sep/09/nsa-spying-brazil-oil-petrobras
28 http://www.reuters.com/article/2013/10/21/us-brazil-oil-auction-idUSBRE99K19720131021
29 http://www.reuters.com/article/2013/09/09/us-usa-security-snowden-petrobras-idUSBRE98817N20130909

Brazil moved quickly to secure its government email systems. A security decree in November 2013 required that:

- Proprietary Microsoft email clients be replaced with the open-source Expresso client[30]
- Government data must be carried by a government organisation or an organisation in which the government is a shareholder, other than for mobile communications;
- The government will create and operate its own email services;;
- Facilities enabling audit of confidentiality, authenticity and integrity of the email system must be built in from the start;
- Data must be stored in government facilities in Brazil;
- Normal procurement practices are suspended in order to get this done without having to seek competitive bids and state-owned IT shops only need apply.[31]

### 2.4 The Brain Drain from Scotland's IT Sector

Scotland boasts several world-class universities, including the University of Glasgow, which has the second-best computer science course in the UK[32]. In the last decade alone, Scotland has produced 48,565 computer science graduates[33].

Yet the Scottish Government estimates that we employ just 73,000 computer scientists, or 15 years' worth of graduates from our universities - and not all of those employed will have degrees.

One factor is that the average advertised salary for a computer programmer in Scotland in Q1 2014 was £37,500, whereas the comparable figure for London was £57,500[34]. Scottish entrepreneurs report moving to London to have greater access to seed capital, a ready market of early adopters, and to be part of London's tech hub Silicon Roundabout[35].

It is clear that the Scottish IT sector suffers from a brain drain. In order to halt or reverse this, the Scottish Government must provide seed funding to Scottish tech businesses, in order to substitute for lower levels of available venture capital, and target new and innovative markets, in order to exploit opportunities for growth.

As Brazil, China and other governments increase their use of open source software to secure their sovereignty, the market for this software will continue to expand. Brazil's software market alone was estimated at $9.48 billion in 2012[36]. There is a tremendous opportunity for Scotland to invest in local production of open source software, halting the brain-drain from our world-class universities and giving us a head start in emerging markets.

30 http://www.actantes.org.br/sites/default/files/gg.pdf
31 http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=2&data=05/11/2013
32 http://www.theguardian.com/education/table/2013/jun/04/university-guide-computer-sciences-it
33 http://www.sfc.ac.uk/communications/Statisticalpublications/2014/HigherEducationStudentsandQualifiersatScottishInstitutions201213.aspx
34 http://www.itjobswatch.co.uk/jobs/scotland/programmer.do
35 http://thenextweb.com/uk/2011/08/28/startup-scotland-the-next-web-delves-into-digital-life-north-of-the-border/3/
36 http://www.nearshoreamericas.com/brazil-beats-china-7th-largest-software-market/

# 3. The Case for Public Auditability

### 3.1 Necessity of Public Auditability

In section 2.2 we saw that even respected companies such as IBM and RSA compromised their products at the behest of foreign intelligence services. Other companies, such as Microsoft, gave the intelligence services early and exclusive access to details of accidental security flaws. Their customers, which included major corporations and governments, were unaware that their software was compromised in this way, because it could not be effectively audited by third parties. Governments and businesses used this software in good faith, unaware that it was broadcasting their sensitive information to foreign governments and, potentially to foreign commercial competitors.

This undermines not only sovereignty, but the internet security that underpins modern commerce. Security expert Bruce Schneier has said, "The NSA's actions are making us all less safe. They're not just spying on the bad guys, they're deliberately weakening Internet security for everyone—including the good guys. It's sheer folly to believe that only the NSA can exploit the vulnerabilities they create."[37]

As the Petrobras case (see section 2.2) demonstrates, access to and security of commercial data is crucial to the maintenance of national sovereignty in the modern world. In this case, the NSA may have compromised the bidding process for oil fields owned by an ostensibly allied country, a serious infringement of sovereignty. It will be necessary for the Scottish Government to take proactive steps to secure government data, commercial data, and the personal data of citizens. Even personal email and communications often contain vital commercial information.

Perhaps unsurprisingly, software open to public audit contains fewer errors than proprietary software. Coverity, a security testing company, found that open source code has .59 errors per 1000 lines of code, while proprietary software has .72 errors per 1000 lines of code - 22% more errors[38].

The post-Heartbleed OpenSSL rebuild (see section 3.3) involved eight lead programmers plus volunteers, and took over 5 months[39]. This five-month emergency effort alone, at the average Scottish programmer's salary would cost £62,000. OpenSSL has approximately 300,000 lines of code[40]. By 2012, a complete operating system was estimated at 419,000,000 lines of code, which would cost an estimated $19bn to recreate from scratch[41].

Most actors, including the Scottish Government, do not have and could not develop the capacity to conduct an effective, comprehensive, and permanent security audit of all the software they use, let alone to correct the errors found. Therefore the only software that can be trusted to handle sensitive data is software that is open to public audit. Public audit allows costs and skills to be pooled between businesses, governments and the security community on an international basis.

Fortunately, there is already a large body of publicly auditable open source software available for use. In particular, GNU/Linux-based operating systems such as Canonical Ltd's Ubuntu and Red Hat Inc's RHEL operating systems are widely used around the world. A wide variety of auditable software exists, including the office suite LibreOffice, which is backed by a coalition of businesses including Google[42], and commercial support contracts and are available for much of this software.

37 http://www.technologyreview.com/news/519336/bruce-schneier-nsa-spying-is-making-us-less-safe/

38 http://softwareintegrity.coverity.com/rs/coverity/images/2013-Coverity-Scan-Report.pdf

39 http://www.openbsd.org/papers/eurobsdcon2014-libressl.html

40 http://queue.acm.org/detail.cfm?id=2602816

41 http://blog.james.rcpt.to/2012/02/13/debian-wheezy-us19-billion-your-price-free/

42 http://www.documentfoundation.org/supporters/

In section 2.3 we saw that Brazil, a key emerging market, is taking exactly this approach to software security.

### 3.2 Case Study: Heartbleed

In April 2014, Neel Mehta of Google and the Finnish security company Codenomicon independently identified an extremely serious security flaw, dubbed the Heartbleed bug, in the open source software product OpenSSL. OpenSSL runs on as many as 2 in every 3 internet servers[43].

Despite its ubiquity, the OpenSSL project has failed to develop a strong funding model, relying on donations and volunteers[44], and employing only one full-time developer, Dr Stephen N. Henson[45]. A commercial arm of OpenSSL was established five years ago, but has yet to bring in more than $1m in fees in a given year. An earnest debate is taking place in the software community about how to correct this funding shortfall.

Perhaps surprisingly, the response to Heartbleed is increasingly being seen as a success story for open source. The OpenBSD community, renowned for their commitment to security, are conducting a full strip-down and rebuild of OpenSSL[46]. This kind of third-party intervention and audit would be impossible with proprietary software.

### 3.3 Funding Auditability

The primary model for funding auditable software is to build a business around it. The software itself can be modified and redistributed without charge, which in the early days led some to question whether it could be profitable. As the marginal cost of all information goods is near-zero, and in a perfect market the price of a good falls to its the marginal cost, information goods function more like public goods than traditional commodities[47], making it difficult to sell software as a traditional commodity.

This has driven the development of service-based business models on the internet, for both open source and proprietary software.

Successful businesses have been built around open source products by providing auxiliary services. Red Hat, the first open source company to surpass $1bn in annual revenue[48], adds value with its ability to turn a collection of disparate open source software into an enterprise-ready, stable package[49].

It seems likely that some projects will not find a business model that works for them. OpenSSL (see section 3.3) is the obvious example. As these often represent critical commercial infrastructure, government funding should be considered - this is a model that already works well for physical infrastructure projects subject to tragedy of the commons effects, such as roads and bridges.

43 http://readwrite.com/2014/04/13/heartbleed-security-codenomicon-discovery#awesm=~oBTbA5HZbMvr7T

44 http://veridicalsystems.com/blog/of-money-responsibility-and-pride/

45 http://www.nytimes.com/2014/04/19/technology/heartbleed-highlights-a-contradiction-in-the-web.html

46 http://opensslrampage.org/

47 http://www.academia.edu/1530512/Wikileaks_Karl_Marx_and_You

48 http://www.eweek.com/enterprise-apps/red-hat-ceo-outlines-linux-growth-strategy.html/

49 http://www.redhat.com/f/pdf/rhel/RHEL6_Advantage_WP.pdf

# 4. Recommendations

A bold strategy to promote the use and production of open source software in Scotland will secure Scotland's sovereignty and grow Scotland's IT sector by producing products in high demand in emerging markets.

### 4.1 Create a national open source transition plan

Scotland should follow Brazil's lead, and create a national plan to transition the country to open source. Urgent attention must be given to critical infrastructure and any computer system important to national security, including privately-held computer systems engaged in commerce of national significance. Given the revelations in the Daily Record of possible spying on MSPs, parliamentary and constituency office computers and telephones must be considered at high risk of attack.

Learning from Munich's experience[50], early phases of the plan would move users to open source applications that can run on existing operating systems, while later stages would transition the operating systems themselves. Legacy single-platform applications could be run on virtual machines.

### 4.2 Amend government procurement legislation to favour open source

Publicly auditable open source software is not available for all software categories, however where it is available it should be strongly preferred. It should be recognised in the procurement process that software is not trustworthy unless it is open to public audit. It should be recognised that the publishing of code under open source licenses is a substantial community benefit.

The term "open source software", in this context, should be understood to mean software published under a license listed by the Free Software Foundation as a Free license[51].

### 4.3 Pay for the open source licensing of existing software

Public sector bodies should, wherever possible, negotiate for existing third-party software to be relicensed as open source. In the case of custom software produced by third parties, a fair price should be negotiated to ensure existing commercial partners within Scotland are adequately compensated for relicensing.

### 4.4 Amend Scottish Enterprise guidelines to better support open source

SMART currently fund R&D and feasibility studies for "a new product or process" that represents "an advance in technological innovation for the UK industry or sector concerned"[52]. This includes commercialisation of innovations already developed in academia. The requirements are interpreted to mean that only software containing brand new algorithms is eligible for funding.

This requirement falls short when funding innovation in information technology. Products such as Facebook and Instagram were innovative when released because of their user interfaces and business models, not their algorithms. New algorithms are often developed by independent researchers and developers across the world, rather than proceeding from academia to commercialisation in the manner of life sciences or engineering.

SMART:SCOTLAND should be instructed to fund the development of innovative user interfaces, the commercialisation of existing algorithms, and the commercialisation of new combinations of existing software.

50 http://www.linuxvoice.com/the-big-switch/

51 http://www.gnu.org/licenses/license-list.html#GPLCompatibleLicenses and http://www.gnu.org/licenses/license-list.html#GPLIncompatibleLicenses

52 http://www.scottish-enterprise.com/services/develop-new-products-and-services/smart-scotland/are-you-eligible

### 4.5 Recognise and invest in critical infrastructure

The Scottish government should establish a stream of grant funding for use by open source projects that it deems critical to Scottish security, sovereignty or commerce and that are unable to support themselves as commercial enterprises. It should lobby for grant funding to be made available at a European Union level for the same purpose.

### 4.6 Encryption by default

All Scottish Government communications should be sent over encrypted channels. Solutions are available for encrypted phone calls, video chat, email and text messaging. These should be used across government, and their use strongly encouraged in the private sector.