FIRSTHAND
realtime data

Intelligence & Security Committee

Privacy & Security Inquiry - Call for Evidence

February 7th 2014.

Christian de Larrinaga
Biography Appendix A

Summary

Assumptions that communications data is safe to pervasively monitor as it can be distinguished from content which is the basis of current practices is not correct.

The use of pervasive monitoring on data networks is compromising individual privacy and as a result is weakening security collectively. Individuals depend on privacy over data communications networks not just to protect themselves but others they deal with including applications service providers such as digital Government services, banking and social networks. Compromising privacy of an individual actor can have implications across the whole.

Actions that undermine encryption are particularly dangerous as they create uncertainty as to the validity and safeness of any service or application either by direct compromise or downstream from it as consequence.

Confidence in UK Government, as well as Parliamentary oversight regarding the safeness of UK data networks as an environment to do business or conduct societally sensitive actions has been damaged. The reasons for this need to be better understood as does any current assumptions that costs of pervasive monitoring are largely zero outside localised points of monitoring and processing.

I realise this is a strong position to take but it should not be interpreted as implying any opinion on legality or good intentions or importance of surveillance. However the costs of current practices do not appear to be sufficiently weighed for data networks. It is impossible from the information available to assess the cost versus risk of current practices.

However I do believe the use of telephony era methodologies for surveillance and legislative backing for this as exists today are not fit for purpose in a data network age. A new era deserves and requires new approaches.

Points

I. I thank the Chairman and members of the ISC for the opportunity to comment on their historic request for input into developing oversight in Parliament over surveillance activities sanctioned by the United Kingdom.

II. My comments are personal and not associated with the Internet Society of UK England which I am a founder (1998) . However the issues are of great concern to participants in UKs Internet communities as they are to Internet communities around the world.

III. As such I recommend the ISC to involve the Internet Society in UK to participate in giving evidence directly to the committee in due course. The local Society is a full voting member of the global Internet Society but as a local body can offer insights from the I* and technical communities independently of any particular sector or vendor interest. A background to the Internet Society can be found in Appendix B.

IV. The questions relating to privacy & security carry some interesting policy distinctions for data networks to those experienced on telephony services. I believe the ISC is correct to ask these questions. I recommend taking detailed evidence on this topic. I think it is incorrect to assume that individual privacy conflicts with collective security. There are many facets to collective security that depend on individual privacy.

V. Privacy is not a stable status. The natural state of information is to be open. To hide information takes special effort. In a digital world where we share data across other devices we own ourselves as well as with people using data networks people notice how hard it is to assure themselves that information remains private and hence secure. It is particularly hard to manage privacy with service providers monetised through social sharing of personal and business data of their subscribers. Their need to share your data is driven by their desire to maximise their profits governed by fear that you will abandon them if they go too far.

VI. Government services to citizens require individual privacy to secure its services to the nation. There is no "collective" security as such in this sense other than in the combined privacy state of all citizens.

VII. The ISC may be referring to a sense that collective security is vested in a national body or intelligence or security agency. There are distinctive threats and risks that are important to be clear about before providing a detailed appraisal of how privacy is impacted. However as a principle the British Government should be promoting individual privacy and only making exceptions where there are clear targeted justifications. Also in recognition that breaches of individual privacy are also breaches of collective security it is also very important that where that is sanctioned and occurs there are effective operational and oversight mechanisms to manage, understand across the government piece and repair such breaches.

VIII. In this sense I support the support GCHQ and other specialists can provide to UK businesses, civil society and individuals in protecting themselves on digital networks and services. It is hugely unfortunate though that this idea is now tainted by the same agencies with their international allies having been discovered to have undermined the same businesses, organisations and individuals security on a massive scale through pervasive monitoring and the undermining of security services in particular encryption.

IX. That activities of pervasive monitoring are a threat to collective security by undermining confidence and just as importantly by undermining the ability of individuals to manage their security with sufficient surety and as such it has weakened protection of society collectively. It is more than an own goal.

X. The Internet technical community has described pervasive monitoring as "An attack on the Internet". IETF Technical Plenary in Vancouver 2013. The precise implications of what this means are currently being determined and the IETF meeting to be held in London in first week in March 2014 is hosting over 2000 of the world's leading data networking engineers. These engineers are being called to strengthen the weaknesses .

XI. IETF meeting follows a two day workshop STRINT (Strengthening the Internet against pervasive monitoring) which is being organised jointly by the W3C and the IAB on 28th February and 1st March. This workshop is attracting leading cyber security researchers to discuss proposals for making the Internet more secure.

XII. The use of language by IETF is meant in a technical sense. It is important to state this clearly. The use of language in Parliamentary and policy circles is also easily misunderstood in other communities. I recommend direct engagement between technical and policy communities to share expertise and intent. I discuss this more below.

XIII. The revelations of the extent of pervasive monitoring has taken the technical communities by surprise. It would be easy to dismiss this as disingenuous given the level of privacy concerns over the practices from some major services businesses operating over Internet networks. However there are important differences to draw between actors operating in the Intenet.

XIV. I am organising a discussion in Parliament in the first part of the first week in March to bring provide an opportunity for Parliamentarians engaged with developing policy including oversight mechanisms for national and policing security to meet up with leaders in the Internet technical community in IETF, W3C and cyber security specialists whilst IETF is meeting in London. Members of the ISC are very welcome and would be able to contribute a great deal in communicating the challenges as they see them.

XV. Data networks take a layered approach in terms of responsibilities for all aspects of their deployment, management and services. This can be confusing for policy makers to appreciate and is a major difference between data networks and telephony networks which are vertically integrated into a single service in a single service provider. Even where there are different service providers competing in telephony services the tendency is for these to be all vertically integrated entities providing the entire wire to call service.

XVI. Data networks are horizontally demarcated with responsibilities segmented at various parts of the wire to application service. This means that each layer has its own signalling or communications data and its own view of content. That data may or may not travel across the entire span of any communications.

XVII. So where a telephony user depends entirely on the security of the telephony service a network user depends on the security of each layer in the service delivery. In practice it is sensible for users to secure their own content through use of encryption as no user can be sure where or who will carry their data from a to b. This is why it is very important that users are able to secure their own privacy.

XVIII. Network services may also encrypt their services at various points in the communication path and this may or may not traverse points of peering or interconnection depending on the layer in the network being secured. They will do this largely to defend their own assets.

XIX. Application services also need to encrypt their services. If you access a Government service on a data network it is important that the communication is secured. The same is true with most online commerce and services any user will use.

XX. Securing through encryption at each layer provides an element of privacy at those layers. Who benefits from that depends on what is being encrypted and for what purpose.

XXI. The privacy of an individual is dependent on that individual being able to maintain some secrecy. This is far from being assured as sharing between people is a principle purpose for communications. The more you share and the more the people you share with who also share the faster your privacy vanishes.

XXII. This is partly why the argument that individual privacy is somehow competitive with collective security does not stand up to scrutiny in a data network environment.

XXIII. Clearly a user of a shared cloud infrastructure is trusting to the security of that cloud provider as well as the sharing policies that provider has with the data that user provides in that service.

XXIV. The Snowden revelations took both users and such service providers by surprise because although it is well known that cloud services push to share as much as their users will tolerate without leaving them the fact that all the data was being snaffled by the US Government and shared with the UK Government and some other countries intelligence agencies was not understood.

XXV. The assumption has been that only communications data might be intercepted and content would only be taken on receipt of a valid court or executive legal order.

XXVI. That the US has made it clear that UK users have no protections at all in the US from their security laws is a considerable problem for these cloud providers. Estimates already suggest a cost escalation of $35 billion for these.

XXVII. My own experiences suggest the UK should also expect economic damage not so much from businesses withdrawing who are already here although there has been some indications of that but from shifting orders for new services to more “secure” jurisdictions by which is meant countries with stronger support for individual privacy. The value of this has not been audited so is not something I would wish to submit to this inquiry. But I recommend ISC takes evidence and research into this issue.

XXVIII. It is apparent that the UK surveillance environment has not taken into account the real costs to users and UK business interests more generally in its conduct. It has very largely assumed that the cost is limited to very few Carrier level service providers that offer space to attach surveillance sinks to underlying infrastructure. That is a not a safe assumption to continue to make.

XXIX. The recent Snowden revelations has shown not just the very broad scope of surveillance but that the cost to society is much higher than has been acknowledged.

XXX. I believe this indicates British surveillance needs to adopt a more standardised risk assessment methodology when deciding on and managing surveillance measures. This risk needs to cost in the potential costs in a realistic way to the general public and society as a whole. Matching threat to risk assessment is something the ISC may wish to take evidence on

XXXI. I also want to add some pointers on why telephony differs technically from data networks from the perspective of implementing surveillance policies and in regard to the current legal and legislative frameworks for surveillance in the UK. The main demarcation for surveillance management is between traffic or communications data and content.

One set of laws are in place for surveillance in general concerning communications data and a more onerous set are in place intended to be used for access to content.

XXXII. In telephony this is relatively straight forward demarcation to make because the communications data travels physically on a separate infrastructure to the voice or content. This is true in your plain old telephone at home as it is between two large carriers interconnecting billions of minutes of calls between each other. (There are some exceptions to this)

XXXIII. Data networks do not work that way. Internet communications data sits at the Intenet layer in data networks. This contains the Internet Protocol (IP) address and application port for the service being used at each side of the communication. Internet Service Providers frequently change these so end points in their networks are not visible outside. This makes IP data unreliable source of intelligence of a user or entity. There are ways to improve this but it will take a change in UK policy towards the national network.

XXXIV. Users are not often aware of the IP layer until something breaks as they use applications and application services. These services also carry communications data as well as content related to that application. These should be encrypted to protect the user from interception by criminals in the network between them.

XXXV. Some application technologies such as RESTFUL interfaces will carry substantial amounts of personal data in the communications data for that application. Other applications will carry threads of conversations such as who is speaking to who within the underlying data. Other signalling data applications hold in data networks include detailed logs of location via GPS or wireless triangulation, biometric identity credentials.

XXXVI. This makes data networks a very different environment to telephony and the rules for surveillance designed to protect deep intrusion of what is said whilst monitoring the details of conversations for telephony are a poor fit for data networks.

Appendix A

Biography of the author

Christian de Larrinaga is chairman of FirstHand where he leads strategic relationships, venture finance, organisational mentoring and public policy. Founder of data communications networks and services since the early 1980s in media, news, financial services and international development. de Larrinaga is responsible for establishing and overseeing wholesale bilateral interconnect and peering services between Internet and telephone networks internationally that support billions of minutes of voice and communications traffic. As a data specialist he has multiple awards for services scoping data visualisations, data architectures, real time information services, messaging and electronic markets. A Past Vice President of the Internet Society he is emeritus founder chair of the Internet Society UK England a past advisor to children charities War Child and Director Internet and Media for Future Trust. He is UK advisor to Wired Safety. He is a Fellow of the British Computer Society and a Chartered IT Professional. He can be contacted on [REDACTED]

Appendix B

Internet Society UK England (http://www.isoc-e.org) is a chapter of the Internet Society. Founded in 1998 it is a not for profit home managed by volunteers for people involved in the UKs Internet communities working in standards, education, research, and policy. With around 2000 participants ISOC England has led or instigated a number of influential projects to improve UK Internet infrastructure, education, policy and research and provides delegates for UK orientated and international consultations in Internet Governance, Standards and development.

The Internet Society (http://www.internetsociety.org) is the world's trusted independent source of leadership for Internet policy, technology standards, and future development. More than simply advancing technology, we work to ensure the Internet continues to grow and evolve as a platform for innovation, economic development, and social progress for people around the world.