PROPOSAL FOR EU LEGISLATION

Mandatory anonymised, authenticated and end-to-end encrypted communications in all telephony and computing devices sold after 201x.

Status: **DRAFT 0.13**

SUMMARY

We suggest legislation to transition to an application of technical measures in electronic communication aimed at a proportionate implementation of the **Secrecy of Correspondence** and **Freedom of Assembly** required by most constitutions and human right charters. The law shall be accompanied by implementing acts and a migration path from the current unsafe communication environment.

„The antidotes against the risk of totalitarianism are [..] weakened to a dangerous extent so that it would not take much more than a spark for the public space to collapse, and this even under the cover of the best governance intentions.“

Nicole Dewandre, Societal Advisor to the European Commission in “the Onlife Manifesto”, p. 195

„At the turning of the millennium, few imagined that citizens of developed democracies would soon be required to defend the concept of an open society against their own leaders.“

Edward Snowden, NYT Op-Ed 2015-06-05

IMPACT ASSESSMENT

Law Enforcement / Cybercrime:

This regulation impedes so-called „cybercrime“ to a large extent: as all communications between citizen are authenticated, it is impossible to deliver so-called „spam“, malware or „trojan horses“ anonymously or attempt abuses like so-called „phishing“ without leaving a trail of evidence.

Law Enforcement / Observation:

This regulation does not impede traditional observation of suspects to be implemented by physical intervention on the *appliances* as long as an observation of more than a fraction of the population is technically impossibilitated. Limits of acceptable observation of citizen are beyond the scope of this legislation and must be specified by Constitution or reasoned by the Constitutional Court.

Electronic Security / Encryption:

Mandatory encryption for communications brings about great benefits for citizen and especially for businesses that would otherwise spend substantial amounts of time and money on communications security, in particular on protection from industry espionage.

Electronic Security / Authentication:

As this regulation introduces cryptographically authenticated communications on all levels, the extremely unsuccessful password paradigm for security can be obsoleted. This provides for a lapse in safety for all remote interaction procedures over the Internet, reducing chances of acts of exploitation, sabotage or espionage based on gaining unlawful access to server systems and saving businesses and citizen valuable time and money.

RECITAL

Having regard to the principles recognised by the Charter of Fundamental Rights of the European Union,

whereas current communication infrastructures deployed in the Union and beyond such as the Internet and digital telephony are insufficiently protective of Fundamental Rights of the citizenry and thus provide a threat to the democratic order of EU member states;

whereas the infringement of Fundamental Rights is not measurable within the digital domain, traditional judicial control over the executive branch thus not possible;

whereas a trust-based delegation of defense of Fundamental Rights to governmental entities is in logical contradiction with such Rights and principles of democratic order and thus not viable;

whereas the bulk surveillance and „big data“ analysis of population activities constitutes a new kind of threat to the ability of the sovereign to exercise its Fundamental Rights free from targeted manipulation which has not been considered by the authors of our constitutions

a loose group of citizen has developed the following proposal for regulation:

PROTOTYPE TEXT OF REGULATION

§§ All *appliances* must at the time of acquisition be fully functional and utilize secret *communication* whenever in exchange with another *appliance.* This intends...

1. *end-to-end encryption;*
2. employing *perfect forward secrecy;*
3. providing *obfuscation* of the identity of the *communication* partners;
4. employing *uniform sizes of resulting encrypted data packets*.

§§ The *appliance* shall not be able or be enabled to disclose private encryption keys to anyone but its legitimate owner.

§§ The vendor of devices shall fully disclose to the public the source code of software utilised to implement the functionality of *communication* and make it anonymously obtainable under an Affero General Public License. (**FIXME**: The explicit mention of a license needs to be replaced by an accurate description of the license's intention. Jimmy may have a suitable definition at hand)

§§ *Appliance* users must be enabled by the device vendors to reproduce the exact binary implementation of functionality of *communication* provided with the appliance from the source codes.

§§ *Appliance* owners must be enabled by the device vendors to autonomously replace the currently installed implementation of functionality of *communication* by another.

§§ Complementing measure shall be taken by implementing act to ensure that no other aspect of the software or hardware of the *appliance* can compromise the primary objective of providing secret *communication*, unless specifically requested by the owner. This includes hardware identification codes and their transmission.

§§ Location tracking of *appliances* and users must generally not be possible. *Appliances* must interact with service providers and the decentralised wireless infrastructure anonymously, including payment methods. Exceptions with the intent of targeted observation of suspect individuals must be confirmed by an independent court and implemented by physical intervention on the suspect's *appliances*. The number of surveilled devices must never exceed one in a thousand per nation. Individuals must be informed within due time of completed observation as specified by national law and given opportunity to restore the confidentiality of the involved *appliances*.

§§ All *appliances* shall be interoperable for the purpose of secret *communication*, using an open standard specified by implementing act.

§§ *Appliances* shall be interconnectable with devices predating their introduction. In this case secret *communication* is provided up to the *gateway*.

§§ *Appliances* that have not initiated *communication* before shall be able to exchange the necessary keys when the owners physically meet and simultaneously activate the *vicinity discovery* function. Alternatively keys may be acquired from a physical print in an openly standardised form to be specified by implementing act, or by the use of a standardised look-up private *network discovery* function. In either case such keys are kept for later confirmation as follows:

§§ *Appliances* that have shared *communication* before, must be automatically capable of exchanging keys, whenever they are in vicinity of each other, without exposing information to *appliances* they have not shared *communication* with before. The appliances shall emanate a standard confirmation sound as the validity of the *end-to-end encryp-*

tion is confirmed or vehemently inform the owners of a constitutional breach (**FIXME**: less dramatic wording?) should the exchanged keys not correspond to previous *communications.*

§§ (**FIXME**: An article is possibly necessary to indicate that a standardised protocol and API could be needed for accessing communication functions of appliances from external, possibly non-conformant devices and how to ensure that the owner is aware and in control of interactions. See below for reasoning)

§§ (**FIXME**: An article requiring encryption of all communication data on the local device long-term storage memory is missing. It needs to clarify that while the device is active and thus in possession of the storage decryption code there must be no way to access it by physical or virtual means – for example by forcing an immediate shutdown when the case is removed)

§§ (**FIXME:** Add an article that forbids communication partners from suggesting or requiring automatic communication with third parties as it could lead to de-anonymisation of the appliance owner.)

§§ (**FIXME**: Provide provisions on the implementation of monitoring of the correct implementation of the law, specifically concerning the involved source codes and hardware specifications, the delivered appliances and the relay node infrastructure.)

§§ (**FIXME**: Provisions prior to taking effect in the year 201x regarding migration and development procedures.)

DEFINITIONS

For the purpose of this act the following definitions apply:

§§ *Communication* means any digital transaction between natural persons or about natural persons that could be of private nature; including electronic synchronous or asynchronous messaging, chat, document exchange, screen sharing, telephony, audio or video conferencing.

§§ *Appliance* means any kind of commercially available device such as telephones, computers or tablet devices that are expected to provide

communication services. Such expectation can be created specifically, but not exclusively...

1. by the fact that the device provides a specific microphone plug or a built-in microphone or a photo or video camera function or any combination of these;
2. if the device is bundled with any external microphone, camera or headset;
3. if it provides *communications* software as defined in this document;
4. if the device offers an easy or straightforward way to install the missing *communications* software.

§§ *Encryption* means "the equivalent to 128 bit key size security" according to the ECRYPT II recommendations on Algorithms and Keysizes (that is at least 3248 bits for RSA and 256 bits for Elliptic Curve Cryptography at the time of writing).

§§ *End-to-end encryption* means that an *encryption* channel is established directly between the *appliances* of the persons participating in the *communication* ensuring that third party or mere conduit can access its content. (**FIXME**: do these kind of definitions already exist in deployed legislation such that we can inherit them?)

§§ *Perfect forward secrecy* means that *end-to-end* encrypted channels renew its encryption keys at least once per day of *communication* or once a week in absence of *communication*. This provides for repudiability and the maintaining of secrecy over time.

§§ *Obfuscation* means that *communication* between *appliances* is delivered over a heterogeneous network of relay nodes in such a way that any third party cannot learn which users are participating in the *communication*.

§§ *Uniform sizes of data packets* means all *communications* are transmitted in form of data packets of standard sizes specified as multiples of 8 kilobytes for real-time data like telephony and 64 kilobytes for asynchronous data like messaging (**FIXME?** too detailed?). Should the data of a *communication* fall below the minimum size it is to be replenished with auxiliary or random data that cannot be distinguished from the actual *communication* data.

§§ *Gateway* means services that interface *communications* between *appliances* and devices predating the introduction of *appliances.*

§§ *Vicinity discovery* means a feature of the *appliance* that allows the owner to learn the authentication keys of another *appliance* nearby.

§§ *Network discovery* means a mechanism to anonymously retrieve the authentication keys of an other *appliance* or an appropriate *gateway* in the case of a device predating the introduction of *appliances.*

// end of actual law proposal //

TECHNICAL ANNEX

Perfect forward secrecy would currently be achieved according to the elliptic curve Diffie–Hellman key agreement scheme, utilizing Curve-25519.

REASONING (FIXME: RATIONALE? WHEREAS?)

It is the duty of the legislators to wisely decide upon priorities; whenever the **Secrecy of Correspondence** is at stake, it must come first over any other consideration. We are aware that this legislation requires massive changes in

- mentality,
- technical understanding,
- development and
- deployment of infrastructure

by the device manufacturers and telecoms, but we are confident the amount of financial opportunity in the European telecommunication market will motivate the necessary development efforts.

We also believe that the **Freedom of peaceful Assembly** has been compromised in twenty years of digital technology. Neither can groups of people meet on the Internet without being traced, nor can groups of

people have a physical meeting out of sight of authorities if they do not leave their mobile phones at home intentionally. The authors of the founding documents of our nation states knew that democracy can only be ensured if healthy opposition and political innovation is protected and promoted rather than surveilled by its government, which by definition has opposed political interests. Confusing the Freedom of Assembly granted to opposition with the threat of terroristic activity is not just an attempt of trading in liberty with security, it is the aim of chasing a threat to public order with an even greater threat to democracy. The governments in power may be acting in best intentions, but they are creating an inbalance in favour of governments to come, whatever their intentions may be.

Remarks on specific paragraphs:

§§ End-to-end encryption is the first step in safeguarding the Secrecy of Correspondence in the digital domain. Since digital data can be processed much more efficiently than paper, it is appropriate to also consider repudiability, forward secrecy, padding and the obfuscation of who is communicating with whom essential to a digital equivalent of the Secrecy of Correspondence as it was intended when it was enshrined in most constitutions and bills of rights. Padding improves protection against statistical analysis which could otherwise reveal what is likely to be contained in the envelope of a letter. Had the authors of our constitutions predicted these technical developments, they would have included them as they contravene the original intention of the constitutions which is to uphold and ensure democratic governance.

§§-§§ Subsequent paragraphs serve the purpose of further protecting the implementation of the Secrecy of Correspondence. Affero GPL is chosen as it is the only established free software license that protects user rights also when the functionality is implemented on a server device, in the case of gateways and telecom service functions (**FIXME**: The explicit mention of a license needs to be replaced by an accurate description of the license's intention .Jimmy may have a suitable definition at hand)

§§ forbids the tracking of movements of devices and thus of the human beings using them as this practice may be considered an infringement of human rights (Art. 3, right to liberty; Art. 11.1, everyone has the right to be presumed innocent; Art. 12, no arbitrary interference with priva-

cy). Options for a human-rights-respecting implementation of billing are discussed below.

§§ and §§ serve the purpose of interoperability between the new network of appliances and its capability to interface with GSM, VoIP and the plain-old (analog) telephony system (POTS).

§§ and §§ implement a Trust On First Use (TOFU) strategy for discovery of communication partners whose only known data is a traditional addressing method such as a phone number, an e-mail address or a full name. The TOFU is checked for accuracy on the first occasion of a physical meeting.

SCOPE – TBD

BUDGETARY IMPLICATION – TBD

IMPLEMENTATION NOTES / FREQUENTLY ASKED QUESTIONS

Formalia: The "§§" symbols indicate an enumeration of articles to be done in an advanced stage of the proposal. "201x" is to be replaced with the year that this law becomes operative. "FIXME" text in parenthesis are annotations reminding the authors of potential improvements.

Frequently experts criticize 128 bits key size as not being sufficient, but "the equivalent to 128 bit key size security according to the ECRYPT II recommendations" in fact, according to Chapter 6 and 7 of the document, means 3248 bits in the case of RSA and 256 bits in the case of Elliptic Curve Cryptography (see Table 7.2 on page 30). The formulation of this specification is indeed quite unfortunate, but it is what the ECRYPT2 group has chosen to use.

A realistic implementation of the "heterogeneous network of relay nodes" for the purposes of obfuscation would function in a similar way to the popular Tor relay network, with the appliances selecting *onion*

routes to their rendezvous points from a random subset of *relay nodes* in a sufficiently low latency distance, heterogeneously operated by telecommunication providers and other institutions.

Mumble over Tor has proven that this can function. Given enough motivation we are positive that the telecoms will find a way to reduce latency within the obfuscation backbone sufficiently to implement telephony in a way that it is no longer trivial to track who is talking to whom. In particular with such a large number of participants and a large number of relay providers low-latency onion routing can be implemented by reducing the choice of relays geographically/topologically.

In a telephony system where the service provider cannot distinguish telephony devices, billing can no longer take place by invasively identifying consumers and tracking their everyday movements. We can identify at least two possible solution paths for a rights-respecting method of billing: (a) flat-rate participation, (b) anonymised micropayments embedded into the onion circuit maintenance allowing for relay nodes to charge a standardised amount per consumed bandwidth. There must however not be a competition among relay service providers as that would stimulate the creation of cheapest routing algorithms, potentially breaching the obfuscation requirement of the law. The owner would thus acquire suitable anonymous digital currency (likely not Bitcoin) and let the devices consume it as necessary. Microfinanced relay node operation is intended to incentivate a diverse group of operators to offer such facilities. The more relay nodes are participating, the more the financial gain is distributed – administrational measures must thus be taken to ensure that this market is open to all kinds of organisations and possibly even private citizen, making the diversity of operatorship of relay nodes a clear political aim for the sake of maximising democracy-enabling anonymity. (**FIXME**: does the law proposal need to articulate this?)

The *rendezvous point* is a relay node which is instructed to register phone numbers and similar data with a privacy-enhanced and sybil-attack resistant distributed hash table (DHT) such as GNS. An other appliance can thus have its rendezvous point look up a GNS entry for that person and enhance in communication over the two rendezvous points.

In the case of a communication leaving the network or coming from

outside the network the respective rendezvous point would in fact be a *gateway*.

The devices should respect the *Entry Guards* concept – that is to maintain a persistent list of entry nodes rather than using new ones at each occasion – for the purpose of reducing the likelihood of choosing both a rogue entry and exit node and thus becoming de-anonymizable by traffic correlation. The *exit node* is either a gateway or the other person's entry node.

This and other aspects do however not need to be specified in the law itself as **the law forbids obfuscation to fail,** thus it is in the responsibility and interest of the telecom providers to ensure this functions in the best possible way. We choose this path since it would not be easy for the legislator to make these choices safely, whereas we do make concrete choices on ciphers and key sizes where we are comfortable that our choices will be safer than of any lobby-influenced group of experts, which already brought us the NIST Standard Elliptic Curves which then made it into the OpenPGP standard – making a whole generation of cryptography tools potentially susceptible to surveillance.

For the purpose of delayed delivery, the appliance can make use of the recipient's rendezvous point to leave data for it. It shall use the key last negotiated via Diffie-Hellman in an opportunistic approach. Appliances must store exchanged keys to persistent memory in order to be able to recover from power loss. It must therefore be ensured that no proprietary device programming has access to this memory, which by consequence means that no proprietary code can exist on the device other than within a sandboxed environment.

All vendors who intend to participate in the future market of communications must thus **release their core virtual machine hypervisors, sandbox environment or operating system as free software** (or employ existing free platforms). Proprietary applications may be provided as guests of such sandbox environments, operating within technologically imposed constitutional limitations. This applies to phones, tablets and traditional computers. Should vendors choose not to release any code, they can offer devices without communication capabilities or channel all communications through a free hardware chip designed to enforce constitutional limitations, similarly to how GSM subsystems are implanted today.

The measures mentioned in §§ would thus most likely be a mechanism of *sandboxing* as currently provided on many appliances by means of a Java™ virtual machine. Any proprietary code must run within such a sandbox and any interference with the core functions of communication secrecy must be impeded. This allows vendors to maintain the established offering of so-called apps.

The number of *hops* in the onion route chosen by the device must be sufficient to hide the identity of the owner of the appliance, yet the owner can choose to use less or more hops (at her own risk if she chooses to use less than the recommended defaults). Real-time communication may be considered sufficiently obfuscated if provided with one intermediate hop between the entry node and the rendezvous point whereas asynchronous communication should travel at least four hops between entry and rendezvous or gateway.

This proposal limits authentication to the moment of vicinity discovery, allowing for a late detection of a possible breach by so-called men-in-the-middle. Authentication methods that imply an extra “bureaucratic” interaction, although the communication has de-facto already been established, have not been considered here, since usability studies have shown their inefficiency. This includes most strategies for shared secret exchange and fingerprint comparison. The proposal however does not forbid owners from using such methods additionally.

The *network discovery* function implements an opportunistic-at-first key discovery backed by the late confirmation technique. We recommend such network discovery to first consult distributed private social graph information, if available, in order to find keys by common contacts between the two communicating persons or entities. As a fallback the aforementioned advanced DHT technology can serve as a distributed worldwide telephone book for public encryption keys.

This regulation challenges and disregards the popular notion that citizen should be empowered to trade-in personal data for convenience or commercial services since the protection of their personal data is frequently, if applied in bulk by so-called „big data“ processing, of constitutional priority itself or because the fundamental rights of third parties (for instance friends and family) are affected. Thus, on the opposite, legislation that punishes data prostitution should be

considered.

KNOWN BUGS

There is a loophole with vendors being able to sell merely Internet-enabled devices that come without communications software, no easy way to install it and no suitable inputs, thus not having created an appliance according to this law proposal. In that case owners can attach some external USB headset and install the software themselves, thus put their privacy at risk. As long as no incentive is given for a large number of people to do this, this is within their personal freedom, as much as any old hardware can be upgraded to operate as a communications device in the new network.

We didn't mention how a telecom provider can offer services other than to offer “service numbers” that the owner can actively “call”. What services would that be? Untargeted advertisements maybe.

Currently this legal architecture does not allow vendors to keep any software or hardware proprietary. This will of course be seen as unacceptable by many players in the industry. One of the FIXME articles intends to incentivate the creation of a standardised access protocol and applications-programming interface (API) such that via Bluetooth, WiFi, USB or other, external devices can interact with the *appliances* and request communication services from them. The software must in this case put the owner completely in control of such interactions, which then serves a similar role to so-called “personal firewalls.” For example a video gaming device oriented towards multiplayer gaming would after 201x no longer be legal as such, but it would need to be paired with the owner's communications appliance before being granted the permission to engage in multiplayer gaming. Similarly, a smartphone as we know it today would no longer be legal, but a tablet device that operates through a conformant communications appliance would be fine. It should (unless I am overlooking something) even be possible that proprietary software and hardware co-exist in the same physical device if the separation is clearly traceable and all interactions pass the obligatory interface, therefore the iOS or Android operating systems would be allowed to exist further as long as the access to network, camera etc remains under full constitutional control of the GNU subsystem.

ANNEX: REFERENCES

In this section we collect references to existing legal provisions, legal definitions, adopted parliament reports etc. We can use these source materials to better phrase our proposal and accustom it to the acquis communautaire. We could also find out which law revisions could be used to introduce elements of our proposal.

– 2001/2098 (INI) Echelon-Report Schmid …? FIXME

VERSION HISTORY

2013-10-26 – 0.0 – conceived by carlo von lynX at #transeuropafestival;
2013-10-29 – 0.1 – draft brought to paper by carlo von lynX;
2013-10-31 – 0.2 – feedback from Christian Grothoff considered;
2013-12-11 – 0.3 – explained "the equivalent to 128 bit key size";
2013-12-25 – 0.4 – language corrections contributed by Thomas Rudd;
2014-09-01 – 0.5 – debate at "Forum against Surveillance," Berlin; subsequent contributions by Jimmy Schulz, Juliane Hüttl, Lester Kortenhoeven, Simon Kowalewski, Christian Pape and Enno Dummer;
2014-09-02 – 0.6 – added reasoning: relationship to Freedom of Assembly, topological onion routing;
2014-09-02 – 0.7 – added article on location tracking of devices, added option of acquisition of keys by QR code or equivalent, explained billing options, relay node incentivation and discovery/authentication options;
2014-09-02 – 0.8 – added FIXME for an access protocol article plus reasoning on proprietary requirements.
2014-09-23 – 0.9 – added FIXME for an article requiring encryption of long-term memory and protection of its decryption code as suggested by Christian Pape.
2014-11-09 – 0.10 – resolved FIXME about inter-appliance communication by changing the definition of "communication" in such a way that it includes data *about* human beings, not just among them.
2015-01-17 – 0.11 – included feedback from Aaron and anonymous
2015-04-14 – 0.12 – included feedback from Andrè Rebentisch, updated a paragraph on sandboxed environments and another on targeted surveillance.

2015-04-27 – 0.13 – added prototype whereas clauses, added unfinished articles that impede online advertising to be based on infringement of civil rights and provide procedural measures for the creation of the infrastructure, added FAQ on data prostitution, first go at an impact assessment.

ENDORSEMENTS

Various organisations are considering endorsing this legislation proposal or a suitable later version or remix. Actual names will appear in a later version, let us know if we have your support.