A Civil Society Glossary and Primer for End-to-End Encryption Policy in 2022

Metadata

This report will be periodically updated to address typos, missing content, missing concepts, other clarifications, etc; a list of diffs/changes will be published for transparency & change tracking.

Contact

- Email: `alec.muffett@gmail.com`
- Twitter: `@alecmuffett`

Version

- This report was generated at:
  - 2022/07/07 12:20:56 UTC.
- Announcement blog post at:
  - https://alecmuffett.com/article/16184
- Latest versions of this report are available at:
  - https://alecmuffett.com/alecm/e2e-primer/
- Version changes are logged at:
  - https://alecmuffett.com/alecm/e2e-primer/diffs/
- Error reports, comments, and requests for additions via email or Twitter, please.
- Consultation queries, personal communications, etc, via email, please.

Table of Contents

Some brief notes regarding style…

Pronouns

This report summarises 30+ years of personal perspective of using and explaining end-to-end encryption, and it would feel *weird* to write it in a neutral, academic style that inflates myself as *we*, unless I am referring jointly to both myself and you, dear reader. Therefore I shall use the personal pronoun *I* where appropriate, but I will not necessarily thereby be attempting to claim sole credit for some profound insight – if any is to be found in this report – just merely the blame.

Reading Order

The goal of this report is for the early material to build a robust and hopefully clear understanding of end-to-end encryption – fixing common misperceptions as we go – and then for the latter, more *quickfire* section to refer back heavily to this context. Therefore I recommend reading the report linearly to assist this.

Alice, Bob, Parties, and Participants

This report deals at length with communication and the identities of the parties who are communicating. For the avoidance of doubt I shall stick with using the usual *"A B C D"* set of cryptographic players, and I will break up their roles as follows:

1. First Party: *Alice*, who is participating in, and sending messages to, a conversation with…
2. Second Parties: *Bob* and *Carol* and *Dave*, etc, who along with *Alice* are all using…
3. Third Parties: Platforms, such as WhatsApp, Signal, Briar, and so forth, under the potentially watchful gaze of…
4. Fourth Parties: Surveillance, both licit and illicit, such as Law Enforcement, NSA, GCHQ, rogue platform employees, and any-and-all others outside of the provision of communication services by third parties to the second and first parties.

Some other thinkers describe all of Alice & Bob (etc) as *first parties*, however I treat them separately due to the *massive importance* which the described approach places upon the role of the first party (i.e. the author or speaker) for each message that is sent.

Foreword

Three fundamental questions have driven the Crypto Wars for the past 30+ years, and they are approximately as follows:

1. should individuals remain free to keep a secret, even from the state?
2. should consenting parties remain free to communicate in a manner that is private, even from the state?
3. should third parties ever be obliged to *not enable* – or even *actively prevent* – access to the above freedoms?

Readers are encouraged to consider the entirety of this report in the light of these three questions. They are key to everything which follows, and I shall return to them in the afterword.

The “Field Model” and the Historical Mundanity of Privacy

It is inarguable that individuals may keep secrets, even from the state. There may be *consequences or punishments* [1] [2] meted out for doing so – or for being *presumed* to be doing so – however every person is de facto at liberty to think or believe whatever they choose within the confines of their own head, and to also (attempt to…) omit or lie to others regarding what they have thought or believed.

Drawing upon this to paraphrase Whitfield Diffie and other encryption and privacy experts and commentators, we can consider the *field model*: [3] [4] [5]

> *Field Model*: All that was once necessary for two or more people to have a private conversation was for them to *walk into a field – away from eavesdroppers* – where they could *simply talk*…

Indeed, as described in the citations and quite intuitively: prior to the invention of parabolic microphones, telescopic lip-reading, wireless bugs and audio recorders, after taking a few steps to stand in a field it would once have been safe to assume that those who could be *seen* as being *within earshot* were the only people who would be *party to* – or *participants in* – a conversation; and of course when standing in that field it would likely have been their *intention* to see who *is and is not within earshot*.

Of course one or more participants might *leak* matters of discussion at a later time, but that would be a failure of trust amongst participants rather than any kind of fundamental flaw regarding the mechanism of having a private conversation in a large arable lot.

Prior to the industrial age this simple act was so obvious and mundane a fact of life, notwithstanding that encryption was widely used (e.g.) during the American revolution, [6] that there was no apparent attempt anywhere to enshrine a robust *“right to agency in private communication”* in any bill or charter of rights – likely because any attempt to do so would appear no more necessary than legislating the right of an apple to fall to the ground if dropped.

Yet far earlier – with the invention of the written word, when it first became possible for *participants* to communicate over a long distance – there were also invented the concepts of *interception* and *censorship* and even *cryptanalysis*, and with those came the notion that it is profane and even incriminating for individuals to attempt to avoid the eye of the state. The canonical example is Mary Queen of Scots whose conspiratorial enciphered communiques were further deciphered and used as evidence against her, ultimately costing her head.

Advancements in technology – creation of the postal service, the telegraph, telephone, radio, internet, etc – have each accelerated the agency and scale of individuals spontaneously communicating amongst each other in a decentralised manner. The state has worked to track technological developments, seeking to maintain its abilities to intercept and censor communication which takes place over a distance:

> In Britain, the General Post Office was formed in 1657, and soon evolved a “Secret Office” for the purpose of intercepting, reading and deciphering coded correspondence from abroad. The existence of the Secret Office was made public in 1742 when it was found that in the preceding 10 years the sum of GBP 45,675 (equivalent to GBP 6,724,000 in 2019) had been secretly transferred from the Treasury to the General Post Office to fund the censorship activities. [7] [8]

… whilst elsewhere technologists have worked to mitigate or undo undesirable aspects of the new technologies which have lent themselves to surveillance, interception and tampering:

> [Almon] Strowger, an undertaker, was motivated to invent an automatic telephone exchange after having difficulties with the local telephone operators, one of whom was the wife of a competitor. He was said to be convinced that she, as one of the manual telephone exchange operators, was sending calls "to the undertaker" to her husband. He conceived his invention in 1888, and was awarded a patent for an automatic telephone exchange in 1891. [9]

Aside: the *directory services* or *impersonation* attack that Strowger feared is today still employed in (e.g.) DNS spoofing and DNS censorship; and as mitigations for these are invented and trialled there is inevitably pushback from surveillance and censorship interests.

We observe an empirical pattern: the state generally permits people to speak privately in a physical space (e.g. *in a field*, where they can be generally observed – by field owners, law enforcement, etc) and sometimes it will to some extent protect this capability (e.g. aspects of *freedom of association*) – however it also invests in undermining privacy of communication over a distance, it combats improvements to the same, and it claims to do so for the most inconsistent of reasons: the security of the Crown, to fight wars, for national security, to combat organised crime, to combat drugs, for the economic [10] well-being of the nation, and (today) to protect children.

It's almost as if they were fishing for an acceptable excuse.

The matter has come to a head since 1975, after development of public-key cryptography after which it is no longer sufficient to have *raw* access to the *medium* – steaming an envelope, listening to radio, tapping a wire, stealing a codebook – in order to enable state interception.

Instead the issue is now with the freedom of participants *to send an arbitrary message* and *to employ encryption to protect those arbitrary messages*. To maintain interception capability in a world of public-key cryptography these two freedoms must be restricted, tampered-with, or suppressed, all to chill or compel aspects of the *speech* via which Alice and Bob would negotiate encryption keys between themselves in a process which would otherwise exclude state oversight.

Public-key cryptography uses processes where participants *actively participate* in *collective negotiation* (and likewise *collective renegotiation*) of the conversation's cryptographic keys in order to enable private communication, thereby empowering the participants to dynamically exclude non-participating [11] passive third- or fourth parties to an extent far greater than that offered by older, static forms of cryptography – such as those used by Mary Queen of Scots, or by *Enigma*-equipped German U-boats in World War II.

These (re-)negotiations may occur infrequently (e.g. once only) or astonishingly frequently, e.g. each and every time that someone responds to a prior message from another participant. This may sound terribly convoluted, but the digital encryption mechanism is conceptually no more complex than an analogue clock mechanism, and each step in the evolution which has brought us to modern protocol design has afforded better security and new benefits.

That participants are still communicating over a fundamentally insecure, wiretappable medium becomes irrelevant other than from the perspective of *metadata analysis* – also known as *signals intelligence* or *who called who, when, how often and for how long?* – disregarding that, the *content* of their communication becomes wholly inaccessible to non-participants.

Most importantly: unless actively policed by the communications *platform* provider, because participants are free to send arbitrary binary messages between each other they are free to partake in all of this amongst themselves – exchanging encrypted messages – without the slightest requirement for "permission."

The most obvious example of this is that Alice and Bob could begin to exchange PGP-encrypted messages with each other via any communications channel: email, tweet, Twitter-DM, WhatsApp message, Signal file-attachment, even USB-thumb-drive-via-postal-service; however there is nothing magic about PGP. Alice and Bob, if their understanding of basic maths was sufficient, could initiate cryptographically-secured communication with each other by shouting across the bar in a pub.

Hence the only practical constraints upon peoples' adoption of public-key encryption are prohibitions of legislation or policy, enforced by punitive sanctions upon platforms which encourage, enable, or commonly fail to prevent encryption from taking place. Even with that: blocking the surreptitious adoption of encrypted speech would be an extremely hard, expensive, intensive, and ultimately fruitless problem to attack.

Perhaps better to encourage it and at least reap the wide economic and privacy-infrastructural benefits. [12]

The Purpose of Encryption

The purpose of any given encryption key is to split the universe into two parts:

1. entities which know the *key* and thereby are enabled to do some or all of read, write, reply, amend, or elide certain content; and…
2. everything else in the universe

Those who are in group 1 would likely consider it unfortunate for anyone in group 2 to come into possession of the key; it would be against their intentions as demonstrated by their choice to use cryptography, and/or to use a platform which uses cryptography to offer the benefit of privacy.

Mary Queen of Scots was doubly unfortunate; she lived in the era of *symmetric cryptography* where encryption was implemented using a static "codebook" which specified fixed secrets (a *key*) and fixed processes (an *algorithm*) for shuffling or representing letters and words, all of which in their static unchangingness were inherently open to being intercepted, theived, replicated or intuited. Related problems plague encryption up to present day, for instance the US Venona Project to break certain kinds of Soviet communications traffic sent between 1943 and 1948, the error brought about by repeated reuse of old codebooks enabling inference of secret key material; or, more recently, undesirable predictability and weakness of random number generation on some Linux systems.

Worse, though, was Mary's own case: she adopted an encryption mechanism which was invented and supplied to her by Thomas Walsingham, the state spymaster who sought to entrap her.

In short: Mary fell victim to a state encryption backdoor:

> Thus Walsingham established a new line of communication, one which he could carefully control without incurring any suspicion from Mary. Gifford approached the French ambassador to England… and described the new correspondence arrangement that had been designed by Walsingham… Gifford submitted a code table (supplied by Walsingham) to [the French ambassador] and requested the first message be sent to Mary. [13]

Aside: This form of entrapment, along with associated "turning" a participant into an informant, is – for the avoidance of doubt – a surveillance solution effective against *all* forms of encryption; and it raises interesting questions of morality and legality depending against whom it is deployed and with which kinds of warrant – a topic which is largely but not wholly outside the scope of this report. Entrapment into a weak or compromised solution is still a common approach to combating privacy amongst criminals and the general populace; see for instance:

1. the FREAK attack to leverage modern weakness of 1990s "export-grade" encryption algorithms
2. the NSA-backdoored Dual EC DRBG compromised random number generator
3. the police-infiltrated and subverted "EncroChat" platform and social network

… all of which constitute attacks upon the privacies of various demographic communities. It is left as an exercise for the reader to determine the desirability of removing privacy from each community, and whether doing so suffers from negative externalities, such as a general loss of privacy, overly-broad impact, or some otherwise unobvious undesirable consequence.

The Intention of End-to-End ("E2E")

For the rest of this report I shall discuss *end-to-end secure and encrypted communication*; for brevity I shall refer to this by the acronym *E2E*.

The intention of E2E is to *restore the model and benefits of two or more people talking privately in a field* – but in a world of *digital communication* where participants may be physically or virtually *separated* from each other.

This goal requires the *exclusion* of message content from all entities who are *not participants* in the conversation – where, exactly as in the *field model* – participation is analogously defined as one who is *apparent as being within earshot of the speaker*.

Inverting this definition we can infer that: if any entity *has access* to a speaker's speech, and yet *was not apparent* to that speaker as being *within earshot* at the time of speaking, then that entity *should not* be considered a valid participant, therefore privacy has been *breached*, and the solution therefore does not offer E2E. This provides a simple falsifiability test which may be used to evaluate claims that a solution is "E2E compliant" and we will explore some concrete examples of this in the *surveillance* discussion, below.

Why everyone should stop talking about "End-to-End Encryption"

It is hard to conceive of an E2E solution that does not use encryption. Perhaps in some steampunk fantasy we could imagine messages being passed via a series of armoured building-to-building *pneumatic tubes* [14] [15] with privacy assured by gas-pressure-based "compromise sensors" and alarms [16] to provide assured private communication; but such would inevitably be limited to niche, privileged, likely Government use as it would simply not scale.

In the physical world it is not feasible to create tamper-resistant direct connections from every home to every other home, for more than a handful of buildings: 10 homes would require [17] 45 direct tubes, 100 homes would require 4950, and 1000 would require 499500 pre-established and security-hardened, alarmed direct "tubes" to be built. Such a physical system is not *scalable* nor *tenable*: inevitably some sort of *hub* and *routing* would be built, spoiling the *end-to-endness* of directly connected and secure tubes.

However there are no such limitations in the digital world.

The universe-splitting public-key encryption parlour trick of *key negotiation* enables two actively consenting participants to trivially construct a secure tube from one to the other *at need*, and they may equally trivially destroy it when no longer needed. An additional parlour trick of *digital signatures* can be employed to obviate Almon Strowger's fear of impersonation, so that the two participants may be assured nobody is acting as an unwanted intermediary hiding inside their newly constructed, *digital tube*.

This construction enables two individuals to define who is within *digital earshot* for their communication – excluding all others – and thereby it fully implements the *field model* for two people; but it also provides a *building block* upon which we can create larger, closed, *private* chat groups of 3, 5, 10… 1000 participants, each of whom will have the same robust cryptographic assurance that the participants *visible* to them [18] are the only people in the universe within digital earshot.

So this is E2E – up to and including socially counter-intuitive notions, like *"establishing a private conversation amongst 1000 participants,"* a concept which some feel stretches the definition of a private vs: a public space but nonetheless is a logical progression holding private the *intra*-communication of the participants who are present in "the field." Because our solution to the *field model* begins with two people and works upwards, *any upper limit* upon the size of a group chat before declaring the chat to be a *public space*, for whatever reason, will be arbitrary and unsupportable on technical grounds. [19] More on this, later.

But from the viewpoint of a civil society digital rights activist in 2022 we are living in very dangerous times for online privacy – and notably we are in especially severe danger from ourselves.

Taken as a whole, *civil society* have spent so many years praising and defending the trees of *end-to-end encryption* [20] that we have largely forgotten to explore, proselytise and defend the larger forest of *end-to-end security* – viz: that which the encryption technology *serves* and which it is meant to *help provide*. Encryption is a *technology*. Communication being end-to-end secure is the *desired result*. Use of the former does not automatically guarantee the latter.

This is a major error on our part, setting us up to be dragged into semantic or architectural, rather than *political* debate regarding privacy. Some who pursue surveillance now call for *backdoors* that provide access to message content *without* tampering with the "clockwork" of encryption mechanisms which protect the message *in motion*. [21]

These proposals are dangerously framed to the media as *"not interfering with end-to-end encryption"* [22] – which may or may not be *technically* arguable – but under such a system every participant in the *field model* would be wearing a state-mandated and potentially abusable listening device, in which case there would be little point to their *standing in a field* in the first place. Instead of surveillance "wiretaps" for a given application being applied in the *middle* – intrinsic to the *medium* of communication – in such systems the wiretaps would be:

- applied at the *ends* via obligatory content-access backdoors implemented on one or more devices comprising each *end*; or else as…
- a supposedly *"ghostly"* extra individual, obliged to be artificially inserted as *an invisible, silent participant* in any "field" where two or more people are gathered together.

Either of these systems (and any variations thereof) defeat the *field model* and thereby defeat the goal of providing E2E.

This would be the endgame for Orwellian surveillance.

Civil society should urgently migrate from a narrow goal of demanding the *feature* of *end-to-end encryption* to the broader goal of demanding end-to-end *integrity* in private communications, inclusive of a right for people to be secure in their digital effects against general communications surveillance, e.g. the state forcing platforms to *break* the E2E *field model* on their behalf.

But this raises an enormous challenge, not least of consistent agreement, consistent perspective, and consistent terminology amongst civil society.

Boundaries of E2E, Boundaries of Ends…

Question: is a person able to have an E2E conversation with their bank?

Some E2E purists would say *no*, but I believe that it's entirely reasonable for a person to communicate with their bank – most likely: their bank's call-centre representatives – by means of E2E channels, and to expect the guarantees of E2E to apply to those communications.

This is a consequence of how one defines the word *end* which is the "E" in E2E/"end-to-end," and in daily life there is a rough and fuzzy hierarchy of expectations, all of which constitute potential *ends*:

1. a particular device, e.g. a specific phone with a globally-unique phone number or other identifier
2. a particular person, who owns/possesses one or more devices
3. a particular company or enterprise which employs multiple people, e.g. a bank with which you deal
4. an outsourced agent of a company with which you deal, e.g. a call-centre which your bank uses

This list is necessarily incomplete and has many edge cases, for instance:

- it would probably be okay for a person to have *type 2* ("particular person") communication with their local vicar or priest (e.g. via a direct WhatsApp chat, possibly including multiple devices) even though the priest is arguably representing a *type 3* enterprise (i.e. "The Church")
- but it would be weird and probably suspicious to have *type 1* ("a direct and unrecorded private line to a particular person") communication with a banker as it might be used to facilitate fraud, money laundering or insider trading
- even ordinary people who believe that they are using *type 1* or *type 2* communication will include "outsourcing" elements of *type 4* (i.e. an outsourced agency of *themselves*) if they have chosen to install tools like Grammarly [23] [24] or other assistant software which will see the *otherwise private text* that they write.

The goal of E2E is to restore the *field model* to digital communication, and I propose that it's within the gift of the participants to choose who they bring into the field to support them; but for the purposes of E2E is it incumbent upon the participants that they reveal who they have brought with them, so that everyone may see that (e.g.) Alice is a user of Grammarly?

No, I do not believe that *that* is an incumbent necessity, for two reasons:

1. Because – as alluded above – this is a matter of "trust" amongst participants, and Alice could equally be screenshotting conversations or leaking them to local law-enforcement on her own. If Alice cannot also be trusted to curate her devices and software to a privacy level commensurate with the discussions that she's participating in, there is a larger problem of trust which is not fundamentally related to E2E.

2. If we assume the converse – that Alice *must* prove to other participants the number of devices she maintains, what third party software is knowingly installed upon them, whether it "exfiltrates" or "backs up" cleartext conversations to third or fourth parties, etc – then we must question whether the requirement that she prove this is *liberal*, *reasonable*, and *achievable*. I aver that it is none of these, especially the latter (provable security) which is one of the hardest problems in security research. If the converse is not tenable, we must assume the proposition. [25]

TCB: the Trusted Computing Base

This approach – that each *end* or *participant* defines for themselves the boundaries of *themselves* and what supporting software they choose to have *within* that boundary – has an existing technical name. In computer security it is referred to as the Trusted Computing Base or *TCB* where the owner of each TCB makes a political decision to (somewhat blindly) trust the contents of their TCB, because they essentially feel that they have no other option. For an Android user this may mean accepting that the Google Play Store will give them a legitimate copy of WhatsApp or Signal, that the keyboard or grammar apps they use will not exfiltrate text to third parties, that the multi-device "Desktop" apps for the chosen messenger may risk but will not by default leak messages via cleartext backups, etc.

The TCB is not part of an E2E other than it defines the physical, virtual and "trust" boundaries of (each) one of the "ends" that participates in an E2E conversation. This also explains how "A Bank, with outsourced call centre" can participate in an E2E chat: because the TCB for "The Bank" encompasses the entirety of bank systems, staff, and call centre.

Some sidebar observations:

- Perhaps I am wrong and somehow it is not reasonable to consider WhatsApp communication with a Bank (and its outsourced call handlers) to be E2E; but if so then responsibility falls upon the contrarian to provide a consistent definition of an *End* for all "real E2E" use-cases. I have not yet found any other definition that works both consistently and reflects user expectations, but I am open to suggestions.
- If a Bank with several thousand employees *can* act as a single end and can participate in an end-to-end encrypted chat with a customer, by what justification would an arbitrary group chat amongst an arbitrary large number of *actual participants* risk being deemed "a public space" and thereby somehow lose status as closed, protected, private group communication?

"Cui Laboras" – for whom is the software working?

The world of E2E which I describe – a world of impermeable digital *pipes* connecting two or more self-constructed and self-defined *ends* of arbitrary size, where metadata analysis *may* be possible and where anonymity is an undefined quality – that world is frankly offensive or considered naive, oversimplistic, suboptimal, or underperformant by some privacy and security activists.

I shall defer detailed discussion of these criticisms to the *Surveillance* and *Interoperability* sections below, but broadly one or more of the following assertions are made:

1. Your definition of an 'end' is wrong
2. E2E needs to address, mitigate, or negate metadata analysis
3. E2E needs to provide anonymity
4. E2E needs to be open source
5. E2E needs to be running on open source platforms

6. E2E needs to be decentralised, distributed, or federated
7. Commercial platforms have no reason to build real E2E, so it's all fakery
8. Real E2E is impossible because [supposed reasons], so give up

All of these are attacks upon the *field model*, or upon *user agency*, or upon *threat models*, or upon two or more of these, jointly; for instance:

- The *field model* has always suffered the risk that fourth parties can see *who* is in the field, and any attempt to change the model simply shifts the problem sideways, e.g. if parties are to meet in a mineshaft in darkness, they may simply be observed entering the mine at a particular time. Mitigating metadata analysis – or its companion problem of avoiding identity-linkage and providing anonymity – requires specialist software like Tor which even then is challenged by timing attacks, [26] [27] correlation attacks, [28] [29] and other end-to-end confirmation attacks. [30]
- If you remove from the user the freedom to define their own TCB then you are obligating them to prove compliance with a predetermined software security policy. In the general case this obligation is *both* illiberal *and* a hard prove-a-negative problem, i.e. *"the user has not installed any risky software."* This risk is greatly exacerbated by regulatory *interoperability* initiatives, in that (e.g.) the parties can no longer be assumed to be using "real" WhatsApp, or similar. Solutions to obtain such "proof of compliance" require pre-existing trust mechanisms such as Mobile Device Management or "MDM" which diminish user agency and open the user to other risks of abuse, including disenfranchisement / being remotely "switched off."
- Demands that E2E software must have a given communications architecture, must be open source, must only run on open source, must be non-commercial, or is somehow simply "impossible" are all versions of the "No true Scotsman…" fallacy. All of these claims are irrelevant to the delivery of data from one self-defined "end" to another self-defined "end" with guarantees of privacy and integrity fitting within a shared threat model. Of course external risks exist – for instance in China the "keyboard app" on your phone may be leaking your keystrokes to the Chinese Government – but in such an instance you are starting with a known-compromised TCB and it is not the fault of the E2E software that you are doing so. Per the "MDM" discussion above, it may actually be illiberal for the E2E software to attempt to override or mitigate your choice of TCB. Instead you should build a different TCB, or adjust your threat model accordingly.
- Saying that E2E is *impossible* because (typically:) *unless the user can personally validate their laptop's hardware, it's impossible to trust software which runs on top of it* – is to deny the user any agency over their choice [31] of "threat model." Someone who is escaping an abusive relationship typically doesn't have to worry about CPU side-channel attacks which leak key material, but they may have to worry that their ex-partner is employed by a platform and might have access to state-mandated "backdoors." The nihilistic slippery-slope towards perfectionism is a common affliction in the world of cryptographic punditry, sometimes to greater harm than good.

This leads us to a question which I call *"cui laboras?"* [32] – for any given software feature we should ask: *"who does this software serve?"* and "how much *agency* does the *first party* have over its operation?"; such agency being one of "can they *avoid* it?" *or* "can they *choose an alternative* that is not afflicted by it?"

I consider the results as a kind of traffic-light protocol:

GREEN Features

The software feature directly serves Alice, the first party; for instance:

1. spell-checking and grammar-checking text (even via some helper-app installed by Alice) or similarly…

2. enabling personal expression through “stickers”; any question of whether Bob should feel *obligated* to (e.g.) install a sticker-pack or CODEC in order to *see* what Alice has sent, is a trust, compliance, and agency issue between themselves as described in *MDM* above.

AMBER Features

The software feature exists to provide *non-compliance-related* [33] value to the Platform, viz: the third party which provides the “field” in which E2E takes place. AMBER features might include:

1. user identity verification via phone number or email confirmation
2. active monitoring of metadata to enable the platform’s “fraud prevention” and “abuse reporting” mechanisms, thereby to maintain the platform’s “safety” value proposition to Alice and Bob.

AMBER features must not compromise the *field model*, but if Alice and Bob do not want them then they are free to choose some other platform that approaches (e.g.) abuse detection differently, or which ignores it entirely.

RED Features

The software features will compromise the *field model*, or exist to offer value to a fourth party such as “the state” or “law enforcement,” or to serve an abstract notion such as “protection of children,” “prevention of terrorism,” or “national security.” Often these features are intended to be pervasive and Alice is intended to have no means to avoid them without inviting suspicion.

RED features may include otherwise-AMBER features that have suddenly become obligatory for legal compliance; this is a reflection of the dual-use problem that (in this case) data collected for a GREEN or AMBER reason might equally be used for RED. Each distinct “intentional use” to which the data is put, ought be considered a separate *mens rea* [34] to the overall data collection’s *actus reus* in the traffic-light protocol.[35] [36]

“But why would a corporation want to deploy E2E?”

Sometimes I encounter civil society disbelief that platforms would want to embrace E2E whatsoever; because surely “data is the new ‘oil’” and “if you’re not paying for it, you’re the product” and “Facebook is listening to you via your microphone” – which means that it would be insane for a platform to intentionally yield access to “private” message content, right?

No. Actually it makes perfect sense for platforms to embrace E2E, to give up access to “private” message content, and the only explanations needed are two words: *engagement* and *scale*.

But before continuing with the economics lesson I *will* share unattributable personal experience: anecdotal rumours *have* reached me of more than one platform attempting to “scrape” private user-content for advertising and sales leads. [37] And it turns out that – in private – most people talk utter *crap* to each other, and the challenges of establishing “meaning” and “intention” *plus* not “weirding out” or “spooking” the users any more than they already *are*, makes for a product with a terrible cost-benefit ratio; and that’s *before* regulators come stomping onto the stage in pursuit of activities which they can leverage fines against [38] the platforms for engaging in.

Those who promote these conspiracy theories generally intersect with those having an inflated notion of the value of individual personal data; some basic maths [39] reveals that individual peoples’ data is not worth very much, so as a business what you don’t want to be doing is undertaking expensive analysis of natural language

when instead you could more simply determine *"this user likes heavy metal music, so let's show her a 'Metallica' advert"*; and (again) this is before considering the new and burgeoning risks of regulatory data protection fines.

But back to economics: the "old model" of messaging is similar to "webmail," founded on the assumption that a platform centrally and by default retains a complete historical record of every message that you have ever exchanged with anyone, and they are expected to protect and store that data indefinitely, until you prune or delete the messages.

This model is terrible for business, and businesses have begun to realise this, especially as people flock to the internet and make increasingly diverse, logarithmic or exponential use of the services. Data was never the "new oil," data is the new toxic waste and for *business* the best strategy is to *not* be the one holding onto data for an extended period. Instead it is cheaper, safer, less risky, and more remunerative to push the burden of message storage, protection, and *availability* back onto the users who sent and received them.

Snapchat was probably the first to capitalise upon the triple advantage of *ephemeral messaging* – at first artificially and poorly, then later more robustly using E2E. By automatically deleting the messages which Alice sends to Bob (or, *everyone*) after some interval or condition is satisfied:

1. Snapchat avoids having to store the data for an indefinite period, possibly "forever"; data centres can be smaller and cheaper, without need for "cold storage" where messages which might never legitimately be accessed again, yet must still be safely and privately kept.
2. Snapchat presents their product to Alice as "more secure" because there is less "digital footprint" – e.g. of embarrassing or salacious partying – which could compromise her privacy over the long term; reduced fear compared to "… what happens if someone hacks your teenage Facebook account when you turn 30 and get a job in politics?"
3. Snapchat receives a huge boost in user engagement – yes, my friends, it turns out that good security, ephemeral messaging and policy-based automated data destruction is one of those "user interface dark patterns" that force people into relentless "screen time" so they can track the *rapidly-expiring* shenanigans and fun which their friends are having without them – and where they can be served targeted adverts where relevant.

Realisation of the third of these explains why "Snapchat Stories" were so rapidly cloned across most other commercial platforms: Facebook Stories, Instagram Stories and Reels, reboots of pre-existing "Status Update" mechanisms in various messengers, the short-lived fad for voice-based social networks like Clubhouse – all software features where Bob *"had to be there at the right time"* in order to see or hear what Alice had done, written, said, or shared.

And, to a first approximation, being there *"at the right time"* means being there *"all the time."*

For companies in the advertising business such a level of committed user engagement is an attractive prospect, especially when it also strongly demonstrates who or what topics are so important to you that you will expend time upon viewing or listening to them.

Deployment of E2E assists the third observation, but it *implements* the first two in the strongest manner possible; as we will later discuss, Snapchat suffered in 2014 when cloud storage used by an unofficial interoperable third party client was hacked to reveal thousands of photos which users had been sharing with each other. This particular risk was mitigated in 2019 when Snapchat moved to E2E protection of images – although message text remains at some risk of interception and hacking, given the user demographics the potential business risk to Snapchat of *text* message leaks is likely much lower than the business risk of *image* leaks – politicians don't use Snapchat to discuss party affairs.

What should “Digital Rights” Civil Society be doing?

If we want to see more E2E – and I believe that we *do* want to see more E2E, practically everywhere – then civil society should:

1. reconsider our approach towards E2E and what it is supposed to achieve for the first and second parties
2. reconsider the “threat models” which we (presumptuously) apply to each platform, whether or not they are implicitly at odds with the platform’s *value proposition* under E2E conditions
3. encourage, even *demand* corporate adoption of E2E *without* compromise of the *field model*, but *with* transparent discussion of per-deployment limitations
4. preserve and encourage *diversity* of E2E application ecosystems

Taking these points in order:

1: Reconsider our approach to E2E…

This has been dealt with above: we should stop lobbying for *end-to-end encryption* in favour of *end-to-end security* including *freedom from mechanisms that enable general surveillance*; and we should recognise that (e.g.) a closed-source platform adopting E2E is *still* a worthwhile goal even if there’s no simple way to *inspect* or *prove* the resulting code.

Assumptions of good intent – and public recognition of the business benefits of E2E – will go a long way in this space, especially since potentially embarrassing reverse-engineering of executables will be forever a thing. An *expanding software ecology* containing increasing numbers of E2E solutions – that is: entire E2E *solutions*, not merely more E2E *clients* for *extant* solutions – drives evolution of E2E technology and offers competitive benefit to those solutions who are willing to engage in greater transparency. Increasing the number of *clients* through artificial “interoperability” programs merely sediments the extant solutions and their weaknesses – making them less likely to adapt, evolve and change, stagnating them, and reducing both user choice and user value.

In short: from an E2E perspective it is better for consumers that startups compete to *build something which is altogether better than WhatsApp*, rather than competing to *build a better user interface for the existing WhatsApp*, because pursuit of the latter:

- will hamper development innovation thereby making a worse WhatsApp for *everyone* in favour of a prototype startup client for *a few*
- will deter development of new, alternative, even radical E2E messaging infrastructures in favour of “Yet Another Combined Client” piggybacking on existing solutions and thereby adding no new security value, except possibly “over-the-top” superencryption via OTR – which might in any case just be a terrible user experience.

2: Reconsider the “threat models”…

We should recognise that there are boundaries for what E2E achieves, that they are less broadly drawn than some believe, and we should *not* demand that platforms try to swallow the entire ocean of cool, trendy, latest privacy-enhancing technologies.

Simply having more *application* of E2E is a good start, and is to be generally welcomed.

WhatsApp is a prime example here, fighting spam and abuse by metadata analysis whilst civil society rages about the business application of metadata without including something like:

> *… admittedly this same metadata – especially aggregated with other, similar data collected on other platforms – can drive valuable anti-abuse features which help protect people and communities at risk from predators, racists, homophobes, fraudsters, and other unpleasant people. These are features that you won't find fully-developed equivalents for on metadata-avoidant platforms like Signal, and users should choose their preferred messenger tool accordingly…*

For the avoidance of doubt, from my perspective:

- it is legitimate and should be encouraged for a platform to make money within bounds of legal operation, especially where they are leveraging E2E to offer value to customers and thereby profit
- metadata should not be considered somehow sacrosanct with people demanding its protection from various AMBER usage on grounds of "preserving E2E"; the goal of the *field model* is to prevent third and fourth party *eavesdropping*, not to prevent third and fourth party observation of who is talking to whom. Actually *preventing* the latter would require *de facto* adoption of new architectural approaches like Tor or Matrix, not *de jure* sprinkling of "log but don't use"-compliance pixie-dust, especially in a world of interoperability
- it is legitimate for a platform to use – or, to choose *not* to use – metadata analysis and other AMBER features in order to offer value such as "spam prevention" and "banning abusers"; however they should be transparent regarding the extent to which they do this, so that users can make informed decisions regards how data *about* them is used, and whether they should go elsewhere for secure communication
- if metadata analysis *also* feeds advertising which eventually pays for the computers and network pipes that support the platform, so be it; but *again* the platform should be transparent regarding the extent to which they do this, so that users can make informed decisions regarding how data about them is being used, and whether they should go elsewhere

If Alice and Bob seek resistance to metadata analysis they should choose a distributed platform which enables that – e.g. Ricochet or Briar. Pushing this responsibility back onto the user(s) is sometimes derided by critics as an "elitist" approach, however as a group we make great efforts to demand that people are able to make *informed decisions*, and this is just another such decision.

3: Encourage, even demand adoption…

"Digital Rights" Civil Society, as a community, has expended much time in the past decade fearing *"corporate surveillance"* of different forms – which has caused us to particularly fret about metadata, wagging fingers, and launching lawsuits at platforms which use or abuse it.

However the goal of E2E is to defeat fourth party surveillance: by the state, by Alice's employer's corporate firewall, by rogue employees of the platform, and so forth; the surveillance which E2E addresses is *not* metadata analysis by the platform, elimination of which requires technical approaches (distribution, mix-nets, …) which is possible but is also beyond the fundamentally obligatory necessities of the *field model*.

In short: if we *also* want freedom from metadata surveillance, we will need to demand *more* than E2E; instead we will need to pursue wholesale demolition and re-architecture of existing solutions, replacing them with alternatives which are dangerously untested at "scale."

This *cannot* be practically achieved by fiat; like it or not, centralised platforms exist and will continue to exist. Attempts to legislatively force their re-architecture will fail whilst distracting attention from, and hampering, adoption of E2E by those platforms – so much so that such would be *welcomed* by those who want to see less E2E.

But pursuing the more limited and achievable goal of encouraging greater adoption of E2E amongst extant platforms, we need to sympathetically refine our thinking – remembering that platforms could *choose*,[40] or are at considerable risk of being *convinced* or *coerced*, [41] [42] to *not* build "real" or "full" E2E at all.

E2E demands restriction of message content access to first and second parties; the platform's *value proposition* or *funding model* may or may not require access to metadata – all of which should be transparent. Telling the platform that they "need to stop making money" will not garner sympathy. Shouting that what they have built "is not *real* E2E because it is profitable," will not build trust.

Therefore to achieve greater adoption, civil society should:

- encourage platforms to build E2E solutions which fit their existing funding models, safety goals, etc
- demand that all platforms be transparent about what they have built, and what boundaries and limitations of its privacy they have implemented
- welcome that some companies will want to deploy E2E solutions and yet turn a profit, so what they build may be less perfectly resistant to (e.g.) metadata analysis than (say) RicochetRefresh or Briar – *and that this is okay*, because the deployment of ever more field-model-compliant E2E is a good thing.

This is a "big picture" matter: addressing fourth party surveillance with E2E is a matter of product design, whereas addressing third party metadata surveillance [43] will require many existing centralised client-server products (and their supporting funding models) to die, so that convergently-evolved distributed tools can fill their product niches. This will require gradual change on a generational timeline, requiring fostering of an application ecosystem rather than regulatory fiat. [44]

4. Preserve and encourage diversity…

Most people who read this report will do so from the perspective of "end-to-end encryption"[45] being a contentious tool that protects messages sent between (obviously suspect) individuals. Others may know it as enabling technology behind "dark web" tools like Tor Onion Networking, or possibly as being the foundation of TLS 1.3, the latest technology to power HTTPS web page fetches – which, just like the other two applications, is criticised by the security services having also received considerable pushback from them during standardisation processes, in various attempts to dilute its security guarantees.

But what you probably don't think of is E2E as the protector of personal information such as your browser activity, credit cards, and passwords.

With all this discussion of end-to-end encryption as if it were some kind of *evil superpower* we can lose sight of its role as a security enabler, and thereby its further role as a *product enabler*.

For instance: if you are "heavy" Apple user, then all your devices are "enrolled" into the iMessage end-to-end encryption system – each of them has a separate cryptographic "identity" but they are all also aggregated under a separate, distinct cryptographic "identity" which relates to *you* as an *Apple user* with an *AppleID*.

This latter is used by and for (not least) iMessage, so that Apple users may message each other with E2E guarantees; per the *field model* above, each user brings into the field their little "cloud" of personally-owned and

enrolled Apple devices.

But given the trust which has been established, those devices can *also* chatter amongst themselves in an E2E manner, and they *do* do so; according to Apple's documentation this tiny little private E2E field is used to share:

- saved payment card information
- saved browser, wifi, and device passwords
- personal keyboard dictionaries
- personalised emoji
- browser history and open tabs
- health and wellbeing information
- … and a host of other data

… privately, amongst all the user's devices.

This data is useful primarily to individuals, and likely none of it (e.g. saved payment card data) is data that *ought* to be available to Apple in its role as a third party "E2E provider" for your devices.

It's notable that Safari Bookmarks are not shared via this E2E mechanism in the Apple system, although they claim at least some degree of encrypted protection; why this is so is unclear, but the lack makes Firefox Sync a more attractive prospect for security-conscious users. Given that Apple until recently have taken few steps towards scanning user content for "badness," my suspicion is that "Safari Bookmark Syncing" probably predates iMessage, certainly benefits from 'cloud backup' and likely lives within a different product organisation inside Apple, so personally I blame this apparent lack upon "corporate inertia."

These products are constantly evolving, for instance Apple recently announced that the same mechanism will be used to share "passwordless authentication tokens" amongst all your enrolled devices; and this – automated proliferation of credential data amongst all the devices that the user has enrolled into their TCB – is arguably a good outcome for most people, for both privacy and security. [46]

Equally: if your Apple Watch can monitor your heart rate and share that data – using the iMessage E2E "personal cloud" – with your laptop so that *you* can track your sleep and exercise regime, all without risking that data being hacked, stolen or surveilled, and equally without triggering a raft of healthcare data-protection legislation… it's pretty clear that E2E is also an enabler of new value.

So let's now pose two questions:

1. Why doesn't Dropbox function this way? With today's technologies it is increasingly valid to ask: *if you want to share a file with a friend, why do you first have to give a cleartext copy of it to a billion-dollar corporation?*
2. If this personal cloud is essentially running on top of iMessage, then what should happen to such personal "clouds" in terms of EU calls for messenger interoperability?

I don't have an answer for the first one, but the second question is particularly pressing: where should interoperability stop?

- Is it immoral that Apple "locks up" your heart rate tracking in a tiny E2E "walled garden" private cloud that only you and a handful of approved Apple applications have access to?
- If so then *why* is it immoral, and *why* should the E2E transport mechanism be to blame?

- And if the E2E transport is *not* to blame, then *which* of your private, personal devices will be the nominated one via which fourth parties will access this private data, and how will *you* guarantee its availability to them?
- Which other novel E2E-data-sharing features are so unique to iMessage that they are "monopolistic?" Perhaps your private and sensitive payment card and health information should be exposed over iMessage to third parties? How will you permit or prevent this?

… and the most important thing about these questions is: they are all equally applicable to E2E "messenger" applications, the ones which the EU are demanding to have "opened up" in the name of "interoperability." There is tremendous potential to break the *field model*, and to distract platforms from delivery of E2E for marginal benefit.

More on this, later.

Surveillance: you can't be "a little bit pregnant"…

Let's briefly review the *field model* one more time:

- Alice is speaking, one of several people standing in a large field. She is the *first party*.
- Bob, Carol, and Dave are listening to what Alice is saying. Alice can see that they are present, and considers them to be *participants* in the conversation, along with herself. Bob, Carol and Dave are all *second parties*, and will themselves take the role of *first party* when they each take turns to speak.
- The field itself is the *third party*; it facilitates private conversation amongst first and second parties, but it has no comprehension of what is being said because fields are meant to be dumb geographic spaces, rather than sentient people.
- That all participants are standing in the field is a simple fact *observable* to (e.g.) the *farmer who owns the field* – and this is a hard problem to solve, going well beyond the scope of "private communication" and treading instead upon "anonymity."
- If any participant should "leak" content to a non-participant it is a matter/failure of trust amongst first and second parties, rather than any systemic problem caused by having a conversation in a field.
- Otherwise: if any non-participant determines a message which Alice has spoken to the other participants, then there *has* been a *failure* of end-to-end privacy guarantees, and therefore *surveillance must have occurred*.

Human beings are not comfortable dealing with hard-edged binary conditions in day-to-day life, often peppering our experiences with arguable provisos and codicils – this wineglass is not *really* broken it's just cracked, that person is not *really* dead there's still a heartbeat – but one of the few hard-to-argue[47] binary experiences in human life is *"you are pregnant"*: either a zygote, embryo or foetus is present in a person's body, or not.

You can't be "a little bit pregnant."

So it goes with the *field model*: you can't be "a little bit surveilled." Either a non-participant has independently[48] determined a message which Alice has spoken to the other participants, or else they have not. If such has occurred, then *surveillance has occurred* and the guarantee of E2E *has been broken*.

What does "determined" mean? In a digital context it is remarkably straightforward to define, perhaps even more clearly than in the real world. A message is "determined" by a non-participant if the non-participant can be certain of the value of *any single bit* of the message [49] [50] [51] with better than 50-50 certainty. One *bit* would be the smallest possible thing that a surveillant could *get*, and this achievement would mean that they had *got*

something. There is a small edge-case here where metadata may expose plaintext – e.g. “yes” is 3 bytes, “no” is 2 bytes – but such *certainty* is generally lost in the noise due to “blocking” factors of symmetric encryption, and other implementation features designed to defeat this issue.

How may we perform legitimate surveillance upon E2E solutions?

There are two straightforward conclusions to be drawn from the *field model*:

1. breaking the *field model* at any point between the ends, must be impossible otherwise E2E is not being provided
2. obligating a mechanism for non-participants to access message content at the *ends* will defeat the intention and benefit of the *field model*, and in any case appears illiberal, invasive, and perhaps totalitarian

So then: how can legally authorised surveillance be compliant with the *field model*?

For a non-participant to read Alice’s or Bob’s messages should ideally require no less than physical access to their devices, having used a narrowly targeted search warrant to obtain that access. Possibly the same can be achieved by targeted hacking – again, it is not the responsibility of an E2E solution to address the existence of malware like Pegasus – but overall the effort required to perform a digital search should be commensurate with the effort required to perform a physical search, and there should be no facility nor support for general warrants.

A bestiary of E2E surveillance proposals

If you disagree with this perspective, consider some alternatives which have previously (or in some cases, have recently) been proposed:

E2E with Key Escrow

In the mid 1990s, much as today, law enforcement expressed fears of encryption:

> “Uncrackable encryption will allow drug lords, spies, terrorists and even violent gangs to communicate about their crimes and their conspiracies with impunity. We will lose one of the few remaining vulnerabilities of the worst criminals and terrorists upon which law enforcement depends to successfully investigate and often prevent the worst crimes.” – *Statement of Louis J. Freeh, Director of the Federal Bureau of Investigation, Before the Senate Judiciary Committee, July 9, 1997* [52]

Computers were less powerful at that time; the typical modern smartphone dwarfs any “supercomputer” of the period, and one consequence of this was that cryptography was used sparingly; keys were generated infrequently, management and authentication of them was implemented in ways which touched upon self-defeat, and regulators proposed to meet the *existential risk* of popular cryptography via means of *key recovery* or *key escrow*, so that the government could feel comfortable in its capability to access any data for which it felt need.

> Under one type of key recovery approach, a decryption “key” for a given encryption product is deposited with a trustworthy key recovery agent for safe keeping. The key recovery agent could be a private company, a bank, or other commercial or government entity that meets established trustworthiness criteria. – *Freeh, q.v.*

The proposal then was that: any time that data was encrypted with a symmetric key, or perhaps any time that someone created a *private* part of an asymmetric *public key* encryption pair, they would be obliged to register (to permit *recovery*, or to otherwise *escrow*) that key with some "trusted" third party authority in case the Government wanted in future to access what had been sent. The following is a particularly egregious UK Government document of the era, from which I will quote a few paragraphs: (*my* emphasis)

> Select Committee on Trade and Industry: Seventh Report
>
> 83. The previous Administration's policy on cryptographic services proposed a licensing criterion on TSPs that they **retain a copy of users' private encryption keys** which could be made available in a timely fashion to law enforcement agencies when appropriate authorisation was provided. The mandatory nature of the licensing regime thus made key escrow a condition of the various attractive services TSPs could offer, particularly the certification of electronic signatures. **Customers could have evaded this policy by choosing to use foreign TSPs.** The previous Government **anticipated this by suggesting the development of an international key escrow regime,** based on existing arrangements for cooperation between law enforcement agencies or new bilateral agreements.
> 84. …
> 85. **Key escrow and key recovery have been almost universally opposed by businesses, cryptographic experts and academics and civil liberties groups** both in evidence to us and in their representations to the Government. The **technical practicalities** of key escrow systems and the cost of developing and operating such facilities **have been questioned** […]
> 86. Critics of key escrow have also focussed on the **civil liberties and privacy aspects** of the policy. **There has been a perception that key escrow, especially if compulsory, would give law enforcement agencies the ability to intercept and monitor citizens' and firms' communications to an unacceptable degree** […]

This deserves some unpacking:

- The goal of this regulation was to forbid people from engaging in cryptography without Government oversight, without Government ability to access message content, etc
- The means of control was to require people to register encryption keys with *Trusted Service Providers* (TSPs) or *Trusted Third Parties* (TTPs) who – the government felt – by their very existence would add value ("various attractive services") to the otherwise simple matter of Alice sending an encrypted email to Bob
- TSPs were to be licenced, and a condition of licensing would be to obey the (key recovery) demands of law enforcement. Non-escrowed encryption would be banned. Users seeking privacy from their own states by using "foreign" escrow, would be caught by international key-recovery agreements. Online there would be no individual privacy, and – since secrets prove identities – very little scope for "trust."
- Proposed TSPs included The Post Office and British Telecommunications which were felt to be trustworthy brands, but nobody seemed to be discussing how the data might practically be protected against (e.g.) rogue or abusive employees of these TSPs, whilst still enabling data ingestion at a huge rate.
- Aside: one of the Government's assumed fringe benefits from this approach is that by artificially creating this industry by the magic of regulatory capture they would please their industry lobbyist friends and could hope to garner huge revenues through taxation; the same playbook can be seen today in the UK's pursuit of Age Verification, including for instance the same safety concerns raised by creating such a huge corpus of sensitive information for arguable benefit

- Any modern enterprise or solution architect would be horrified to look at the escrow/recovery proposal. Newer and more powerful computers – and better algorithms – mean that new encryption keys are generated and used every time that someone presses the *Send* key on their messenger, or a dozen times every time a web-page is refreshed, rather than when you move university or employer and get a new email address
- Even if it were liberal, escrow would not have worked – TSPs and TTPs would have been long-ago swamped, or alternatively we would all be ignoring the law and using software unencumbered by pointless middlemen
- If nothing else this lesson should underscore the critical importance of not permitting legislators to regulate the *shape* of software architectures, rather than their *intention* and *use*

The above-cited report was written in May 1999; by October the proposal was dead but still writhing, and reading between the lines of the subsequent report is darkly amusing, yet still worrying: (*their* emphasis)

> 1999 Select Committee on Trade and Industry: Fourteenth Report
>
> 13. We are concerned that the Government has yet to rid itself of its previous attachment to key escrow and related technologies. **Rather than rule out key escrow because of the wide range of criticisms made about it by industry, civil liberties campaigners, computer experts and others, the Government has simply admitted that its widespread adoption is unlikely at present.** We recommended that powers should not be taken in the forthcoming Bill to permit the introduction of key escrow or related requirements in future, for instance by an addition to the accreditation criteria for TSPs if a statutory regime were in force, but the Government chose not to answer this point. **We are also concerned that although a mandatory link between approved TSPs and key escrow has been ruled out, the Government might encourage a voluntary link instead. The Government is likely to make use of TSPs in its electronic communications with firms and individuals and might seek not only to deal with accredited TSPs but with TSPs which offered key escrow or related services as well.** A recent report by the Performance and Innovation Unit of the Cabinet Office suggested it was likely that the authentication and encryption standard adopted by the Government would "become the de facto UK standard". By working only with those TSPs which can provide key escrow or related services, the Government could encourage the widespread use of such services throughout the UK.
> 14. Following on from the Government's welcome announcement that key escrow would not be proposed as an accreditation criterion for TSPs under a statutory regime, but in the light of the concerns we have outlined above, **we recommend that**:
> - **the legislation should explicitly exclude the use of key escrow as a criterion for accreditation under a statutory regime**
> - **key escrow, key recovery or related measures should not be accreditation criteria under an industry-led regime**
> - **if it were decided to seek to introduce key escrow, key recovery or related measures in future then the accreditation scheme should be placed on a statutory basis, if it were not already so, and there should be provision for a full public consultation exercise and parliamentary decision on the issue**
> - **an unequivocal commitment be made that key escrow, key recovery or related measures will not be introduced through the back door as a result of the Government's participation in electronic commerce.**

It is notable that the Government department's *own* committee felt it necessary to attempt to slam the door shut upon unofficial or "backdoor" attempts to bring *key escrow* into existence by means of compliance for Government contracting.

This is now history, but it is also a microcosm of where we are today: Governments proposing huge changes and vast infrastructures with intermediaries, costs, and choke-points upon performance, all of which we have done without for 25 years and yet somehow have still survived.

Summary: *key escrow* and *key recovery* provide message content to entities beyond the participants, therefore they break the *field model* and so break E2E.

E2E with Message Escrow

Message Escrow is probably most commonly encountered as a joke: a politician or civil servant says something illiberal or misconceived regarding internet surveillance, and some wag or troll says that in future they are going to send carbon-copies of all their emails to the President, the Prime Minister, the head of the Security Services, or similar.

But as a means of surveillance it will help us with subsequent discussion and is delightfully easy to explain:

Alice sends messages over cleartext to Bob, and then stashes a copy of her messages (and of Bob's replies) where then can be obtained by fourth parties

If Alice is aware that all this is going on and is okay with it, then this is all part of her TCB, it is a GREEN feature, it passes the *field model*, and so E2E is preserved.

However: if Alice's (and Bob's) data is (at risk of being) leaked to fourth parties without Alice's or Bob's knowledge or consent, then *that* aspect of the system becomes RED and E2E has been broken.

Hence why implementers should strive to build their software – at least: the aspects of Alice's TCB which they reasonably *do* have control of, such as the E2E application design and data storage architecture – so that it is hard for GREEN features to trivially be turned RED.

E2E with Message-Hash Escrow

The Indian Government is greatly concerned by WhatsApp, and especially wants to be able to trace the 'originator' of much-forwarded viral content within an E2E system such as WhatsApp.[53] [54]

To this end, rather than Message Escrow (above) they propose that WhatsApp should apply a hash function (also called a message digest) to each message that a person composes, where the "hash" is a irreversible digital fingerprint of the messages's plaintext content, whilst also somehow separately encoding and storing the identity of the person who initially composed that message. The hash-and-identity originator information would be left unmodified if the message was merely *forwarded* by Alice to Bob.

> "All we are saying is store the hash, identify it for a particular message and tell us the originator for the same as the value is constant," the official said. "We do not even want to know who all the message was [sic] forwarded to."[55]

There are a number of problems with this scheme: hashes are fragile and even the act of saving-and-resending an image may create a new hash due to changes in EXIF data or automated image resizing, there's no guarantee that the originator of the message being pursued is the actual originator. When this is eventually

noted, it is likely to bring about compensatory surveillance of a more extreme sort.

Worse and more immediate, however, is that this proposal replicates the existing weaknesses of static password guessing, – that all an attacker needs to do is guess a plaintext (e.g. *I'm pregnant.*) – or synthesise one within the platform – compute or obtain the hash for that message, and demand a search of the database for senders who have previously sent a message with that hash. This mechanism leaks message content beyond the participants, breaks the *field model*, and therefore breaks E2E.

Ghost Protocol: your invisible friend

In a 2018 Lawfare blog post, [56] representatives of GCHQ proposed a new twist on key escrow; that platforms should be obliged, when hosting an E2E conversation, to splice an additional and invisible participant – this participant is referred to as a ghost, [57] but more traditionally she is named Eve, the eavesdropper – into the conversation. Then at some later juncture, if lawful surveillance was required, law enforcement could simply consult Eve.

However: the *field model* requires that the First Party (Alice) must be able to *see* and be aware of all participants who will hear or receive what she says; having an invisible participant breaks the *field model*, and therefore breaks E2E.

GCHQBot: I ain't 'fraid of no ghost…

Prima facie the GCHQ *Ghost Protocol* only breaks the *field model* by dint of being invisible to the participants; one solution to this is obvious: the *ghost* should be made into a real and obvious full participant. Each and every chat – however small, even those which are E2E *Notes To Self* for one user only – would be seen to include *GCHQBot*, or *LawEnforcementBot*, or similar.

This proposal may sound flippant but by comparison UK automotive speed cameras are meant to be visible so that they are less open to abuse as a means of revenue generation; this is not obliged by law but public reaction against *hidden* speed cameras was considerable, because hidden cameras fomented public fear of authority rather than deterrence. Similarly, there are significant obligations on UK CCTV users to inform people that they are under surveillance, amongst other requirements.

As such we should ask the question of what law enforcement *would like to achieve* by means of ghostly surveillance – is it not deterrence? If it is *not* deterrence, then why not?

And if the goal *is* deterrence, then why not be *overt?*

E2E and extra-application scanning

Posit:

- Alice has an iPhone
- Alice has WhatsApp
- Alice has configured WhatsApp to save all incoming images to her iPhone *Photos* (formerly known as: *Camera Roll*)
- Alice's Photos are automatically backed up to iCloud
- Bob consensually sends Alice some intimate pictures
- Somebody hacks Alice's iCloud account and steals the pictures

Does this break the *field model*? No, distinctly not. Alice made several choices within her TCB:

- the choice to use iPhone
- the choice to use WhatsApp
- the choice to auto-export photos to Photos
- the choice to back up to iCloud
- the choice to use a poor password and/or not enable two-factor authentication

All of these choices are within her TCB, have been curated or controlled by Alice, and she bears the responsibility for the leak.

However: from a civil society perspective this is a tremendously important example because it highlights the *different* illiberality of Apple's recent CSAM-detection proposals:[58] [59] [60] [61] [62] none of the privacy risk was related to E2E, and the *field model* was not even relevant to discussion.

What we could and did do in this circumstance was to ask *Cui Laboras?* and determine "Who does the software feature serve?" – and the answer would be:

> RED Feature: The software features … exist to offer value to a fourth party such as "the state" or "law enforcement," or to serve an abstract notion such as "protection of children," "prevention of terrorism," or "national security."

I feel that there is scope for much discussion of *Cui Laboras?* as a tool to help decide whether software serves a liberal end. If a person buys a phone or laptop it seems reasonable that the features of the device serve the interest of the purchaser (i.e. GREEN) or the interests of the platforms from which the user derives benefit (i.e AMBER) rather than serve some fourth party (i.e. RED).

E2E and intra-application "client-side scanning"

The European Commission proposes an anti-child-abuse surveillance regime which is stark in its illiberality grounded in arguments which cite increases in (important) *reports* of Child Sexual Abuse Material (CSAM) – report numbers which at a minimum are inflated by perhaps between 75% and 97% of duplicates and not-maliciously-intended content as reported by Meta – the largest "reporter" – themselves.[63] [64]

The proposals are phrased in terms of obligations of outcome rather than obligations of technology, and they pursue the following goals:

- Option A: oblige means to report, make attempts to prevent/detect abuse occurring, and provide victim support; depending upon interpretation, this seems fair and sensible
- Option B: oblige voluntary detection of known content, with mandatory reporting & removal; again, this is not uncommon amongst centralised platforms
- Option C: oblige *mandatory* detection of known content, with mandatory reporting & removal
- Option D: oblige *mandatory* detection of *unknown or suspected* content, with mandatory reporting & removal
- Option E: all of Option D, plus unspecific *grooming detection*

All of these, especially the latter three obligations to be delivered in a manner so they cannot be "misused".

I have written at length on Twitter regarding this proposal [65] [66] but for the purposes of this report it is straightforward to observe:

- *reporting* of content (known or unknown) breaks the *field model*, and therefore breaks E2E

- *detection* of content (known or unknown) which somehow leaks even one bit – for instance: this image does/does-not match one of a set of banned images; or this image does/does-not trigger this image classifier – in a way which can be observed by a non-participant, breaks the *field model*, and therefore breaks E2E

For the avoidance of doubt:

- all *client-side scanning* which affirmatively or negatively reports to a non-participant regarding the nature of content, is thereby leaking at least one bit of information, breaks the *field model*, and therefore breaks E2E.
- all claims that *client-side scanning* can be justified by *discriminating* and restricting it to *"only search for bad stuff"* are ignoring that the feature is a general-purpose Pandora's Box, and ignore the lessons of (e.g.) the Regulation of Investigatory Powers Act (2000) which was designed as anti-terrorism and anti-organised-crime legislation, but is now used to surveil suspected fly-tippers, benefits fraudsters and parents who lie about their school catchment area. Most likely the first step down the slippery slope would be pressure to use the feature *also* to detect copyright infringement [67] [68] – but this is a topic already extensively explored in Abelson et al's Bugs in our Pockets.

E2E and full-device "client-side scanning"

It should be noted that the illiberality of the previous is even more magnified in discussion surrounding their proposal – specifically in the impact assessment report – which includes (my emphasis):

> The detection tools could in principle be incorporated either at the app **or the operating system level** (although in the latter it could be more technically complex). It might be easier for the ESP to check against manipulation of the detection tools before allowing the operation if they are incorporated at the app level but **incorporating the solutions in the operating system may be more effective and efficient to implement.**

… where they are literally proposing the addition of ostensibly anti-CSAM, but practically general-purpose (e.g. copyright infringing) content-surveillance and censorship into core Android and iOS platform software; on the grounds that it would *automatically work for all apps* and *be harder to circumvent that way*.

Such a feature would likely be implemented as part of the operating system *text*- and *image-rendering* code – foundational APIs and services which permit apps to (e.g.) request that the operating system:

> …take the text "hello world" and put it onto the screen in purple 30pt Helvetica in [this] closeable window that I previously created, placing it at X/Y offset 100,120

Except for very-specially-privileged ones, *all* apps are required to use standard APIs to access shared resources such as placing text on screen, writing data to storage, and so forth. As such they provide an obvious potential point of control where the *text* or an *image* that an app has requested to show on screen can *incidentally* be run through a *naughty-word-detector,* [69] [70] or can be thrown at a machine-learning classifier to check if it is potentially suspect, perhaps triggering mitigation-handling like text redaction or image blurring or even automated logging/recording and reporting to the authorities.

But *unlike* intra-app client-side scanning, if embedded into Android or iOS as a core feature then *all* of this filtering would happen automatically for *all* apps, or perhaps only those which *lack certain privileges* or which have been *singled-out for special treatment.*

That states would pursue surveillance capabilities in general purpose operating systems has always been likely [71] but it's astonishing to see the EU at the front of democratic states demanding such.

If such features ever become widespread the important question of who oversees the contents of the blocklists, who oversees the models used for image or sound classification, and how platforms will reconcile multiple governments all demanding that *their* blocklists and models be used against [various user demographics]… will be a significant question of *surveillance compliance. (q.v.)*

E2E and platform behavioural metadata analysis

Typical claim: *Facebook or WhatsApp can spy on WhatsApp metadata, which breaks E2E!*

No it does not.

The *field model* has *always* suffered the risk that third and fourth parties can see *who* is in the field, and any attempt to change the model simply shifts the problem sideways, e.g. if parties are to meet in a mineshaft in darkness, they may simply be observed entering the mine at a particular time. Mitigating this risk requires specialist software like Tor which even then is challenged by timing attacks, [72] [73] correlation attacks, [74] [75] and other end-to-end confirmation attacks. [76]

We should not be complacent nor blase about metadata, but nor should we make overbroad claims that surveillance of metadata impacts E2E. WhatsApp use just such metadata analysis to combat spam and abuse; and in the process they use *behavioural metadata analysis* techniques – looking at *metadata over time* – similar to those which intelligence services for years have used to track criminal gangs. [77]

Similar but more likely *static* (*"… Alice is a member of a Metallica fan-group or group-chat…"*) metadata analysis for Messenger likely provides advertising revenue which (in part) pays for the computers and networks that *provide* WhatsApp and Messenger.

It would be good for civil society to ask itself whether it wants E2E to only be available via boutique applications which run on donations and charitable funding, and which lack niceties such as scaling to billions of users, attractive user interfaces, rich content, and active anti-abuse and anti-spam working to meet the demands of such a large user base.

E2E, entrapment, and honeypots

The platform and social network EncroChat marketed itself as an E2E solution. It was not. It was also primarily marketed to the criminal fraternity, and was a form of honeypot or sting operation with the goal of enabling mass arrests.

EncroChat clearly broke the *field model* and therefore broke E2E. Is this a matter for civil society? I think not, and rather it's a matter for trading standards or other consumer rights and advertising standards organisations, where an impacted user wishes to bring a case.

Flippancy aside: for this to become possible, however, requires the standardisation of the *field model* and its associated test, in measuring whether a given offering truly supports E2E.

E2E, signals intelligence and bulk interception

Posit: Bob receives a E2E message with a link that looks something like:

`https://example.com/click?jjfdqpfmgta5n5mglgiu7j`

Question: if he clicks this link, is E2E being broken?

This is a subtle question to answer, and the answer can be both yes and no. Clearly the link has been composed with a random nonce (i.e. a unique string of letters and numbers) which would facilitate tracking, such that someone observing the logfiles of `example.com` would know that the message Bob received contained `jjfdqpfmgta5n5mglgiu7j`.

Naively we would say that this means that data had leaked, therefore the *field model* was compromised, and E2E was broken; however:

1. It required an intentional action by Bob, within the boundaries of his TCB, to act upon this message and reveal himself. He *owns* this action, rather than it being a function of the E2E solution.
2. A weaker argument also exists, that whoever sent the message to Bob already knew what the nonce was, probably runs `example.com`, and therefore no net information was leaked; but this makes unwarranted assumptions and in any case is weak, e.g. other people might *also* be able to read the logs for `example.com`. It's better instead to simply acknowledge Bob's agency and culpability.

One could make an argument like *E2E should always prevent links being clicked* – but that would defeat the point of Alice sending a *URL* to Bob in favour of:

- presuming that Bob does not realise the risk, or
- ignoring that Bob may already mitigate this risk by using (e.g.) TorBrowser.

E2E client software which pretends to care about offering credible anonymity should perhaps offer a one-time "Don't show this again" dialogue warning Bob that clicking links may cause him to "out" his identity, but this is not obligatory for E2E *per se*.

However: if the E2E platform pre-emptively wraps Alice's URL in some sort of link shortener (Twitter's `t.co`, Facebook's *Linkshim*) and/or inspects the URL content "pre-flight" for signs of malware, etc, then *yes* the *field model* and E2E have been broken, because the URL *was* message content which leaked beyond the participants.

So it goes with most (all?) forms of bulk interception and surveillance; provision of E2E is a function of delivering the *field model*, and nothing more. Elsewhere there may be cryptographic risk which mass surveillance and interception makes worse [78] but these are much less pressing in modern E2E with its heavy dependence upon frequent, stateful change, and active participant participation in key re-negotiation.

Applications where bulk interception or other forms of metadata surveillance which use a *godlike perspective* to operate, may simply benefit from adoption of a different network stack.

E2E and accidental logging

Every so often in a software engineer's life, they will do something amazingly stupid. A shining example of this was at Facebook where – as I know *exceedingly well from a personal perspective*[79] – the security of plaintext passwords is taken phenomenally seriously, with great effort poured into *doing the right thing for protecting that data*.

And then someone working on code *upstream* decides that it makes sense when (e.g.) some exceptional condition gets triggered, to just log everything, after all, what could possibly go wrong?

Answer: they could leak security data.

The same thing is entirely possible within mobile apps which deliver E2E; eventually one of them will buggily "leak" messages to logfiles where the messages could be seen by non-participants and therefore break the *field model*, thereby breaking E2E.

But is this a backdoor? Probably not intentionally. But it's most certainly a break in E2E, and if they want their offering to be credible then they should avoid complexity and leaking diagnostics.

My opinion is still undecided regarding logging systems based upon differential privacy; my gut feeling is that they offer the opportunity for platforms to make rods for their own backs, adding metacomplexity – … *how do we do logging for the differential privacy code?* – and are at risk of if you build it they will come syndrome, attracting those who will demand use of this apparently "privacy preserving" technology for social purposes and to gain political leverage.

E2E and "application usability" within the TCB

A few years ago the Guardian ran a breathless piece claiming that there was a backdoor in WhatsApp; drawing a substantial backlash from technologists, the piece was subsequently reworked and was reported upon by their public editor.

The purported *backdoor* was this:

- if Alice sent a message to Bob…
- but before Bob received it, a different phone than the one Alice had composed her message to, was (re-)registered with Bob's number; perhaps Bob's old phone died, or perhaps he is a dissident subject to interference attacks…
- then Alice's WhatsApp application would retry and resend the message to the new phone without first checking with Alice.

How does this fit with the *field model?* Surely this is a leak?

Actually it's within the *field model* because – whether or not it's a particularly *informed* decision for the participants to have taken – WhatsApp and all of its behaviours are within the participants' respective TCBs.

The virtual identity (or: *identity principal*) that WhatsApp users take into the fields with them are actually *phone numbers*, not human beings, not driving licences, not passport numbers.

Phone numbers when used as identity principals are subject to certain risks [80] [81] and it's up to Alice and Bob whether they want to live with those, or to choose a different solution. This is no more a backdoor than *backing up your messages in unencrypted cleartext to Google Drive* would be a back door; but you are not and must not be obligated to back up your messages in cleartext, nor are you obligated to use WhatsApp over any other tool.

Caveat emptor, and all that.

Also: WhatsApp have since introduced two-step authentication PIN numbers (subsequently followed by Signal) which for a seven day grace period prevents non-participants from (re-)registering themselves with an extant participant's stolen phone number. Hopefully this is long enough to detect and warn participants of malicious activity.

E2E in Civil & Human Rights

Limiting Digital Assembly

Here's a thought experiment:

Imagine that legislation is passed to cap the maximum *size* of a private[82] E2E conversation with an arbitrary limit, for instance stating that *30 people* [83] would be considered "too big?"

But from the perspective of the software, what does *30 people* mean, and how could it tell?

If each person has between 3 and 5 devices – *personal phone*, *work phone*, *still-enrolled but dead old phone*, *tablet*, *kid's tablet*, *smartwatch*, *laptop*, *desktop* – that cap will be exceeded in fewer than 10 people, perhaps as few as 6.

The boundaries of cryptography don't necessarily relate to *people*; if instead of *counting devices* one person with two *phones* joined both of those phones into a WhatsApp conversation, would that count as 1 person or as 2 people?

And how would the software know that? Because (again) some software will see *phone numbers* rather than *people*.

What pointless burdens would we place upon chat-group administrators to plead with participants not to add more than one device to the conversation, in order to free up a privacy "budget" to accomodate more people?

Would helper *"bots"* be counted as *people* towards that budget of 30 people? What if the bots were powered by "Artificial Intelligence?" Perhaps 50 would be a better limit? Or 100? Or 500?

But if 100 or 500, why bother limiting at all?

At the other end of the scale: what means would be deployed to prevent several school children – or *terrorists*, same thing – from communicating by binding multiple, individual "desktop apps" to a *single* phone's messenger app? There are many precedents for creative private communication where it is not straightforwardly provided. [84] [85] [86] [87]

The law – and legislators – tend to presume that unitary physical world identities somehow have one-to-one mappings in the digital space, and that there exists some meaningful digital concept of *too big* or *a theaterful within which someone should be* restrained from shouting "fire".

This is not correct, instead digital identities are birthed simply by creating a new account, or by requesting a new cookie, or by generating a new cryptographic key, and all are disposed of equally simply. The ability to do this is not tied to any obligation to register or escrow the identity, and bizarrely while some parts of government(s) are attempting to create such an obligation [88] [89] other parts which fear corporate monopoly more than going dark are gradually building conditions for distributed messaging which will make it impossible to centrally control identity – although they have already identified that risk and are working to mitigate it. [90] [91] Nonetheless: central control of digital identity is disastrous in the short term, and impossible in the long.

Why? Because lawyers invented the entire world of copyright and trademark so that privileged people could claim ownership over words and content.

But nobody asked the words what *they* wanted.

Trademark and copyright act in one direction; it is not possible to walk up to a paragraph and ask it *"excuse me, who owns you?"* – because a paragraph is an abstract block of data that has no concept of *ownership* other of that which is literally *presumed* by supposedly *authoritative* top-down ownership metadata written *elsewhere*: a register of trademarks, a copyright library, the frontispiece of a book. The thing which is owned is disjoint from that which claims ownership of the thing: people may claim ownership of data, but *data* does not assert who owns it other than by resorting to *metadata* which may be wholly ignored - compare the who screencapped my NFT? phenomenon.

Therefore until the law somehow *obliges the creation of ownership metadata for all data* – a process which if centralised will cause a vast performance sink, and if distributed will be inconsistent, flaky, open to conflict, or simply ignored – there will never be robust linkage between physical and virtual identity. Legislation obligating owner-registration of all identity principals [92] will lead to an *authoritarian ratchet* where there will only be software that is onerous and requires a driving licence or passport to set up; or else whatever competitor that will eventually replace it *and does not*. The latter will eventually become the former and a new challenger will arise.

This disjoint relationship between physical identities (one per *corpus*) and virtual ones (potentially legion, potentially entirely unattached to physical identities) will never be *solved* because they are in the nature of data and communication as a *space of speech.*

As such, all concepts of "limit" in *digital spaces* are essentially arbitrary; in computing this is known as the *ZOI*, or *Zero-One-Infinity* Rule, which:

> … argues that arbitrary limits on the number of instances of a particular type of data or structure should not be allowed. Specifically, an entity should either be forbidden entirely, only one should be allowed, or any number of them should be allowed. [93]

All online arbitrary limits eventually just run into irrelevance or impossibility; it would be far better instead for legislators to address *intents* and *activities* and *behaviours*.

Surveillance Compliance

Imagine a world where countries, states, governments have obligated all platforms to insert backdoors into their messenger software to serve surveillance requests by those countries.

Who will arbitrate the question of which users of what nationalities, resident in which countries, may be surveilled by which requesting governments?

The security services of the different countries will fight with each other for intra-corporate dominance, pursuing the power to filter and veto platforms from honouring exceptional access requests from competing countries, on the basis that such may empower corporate espionage.

Such an obligation will drive a deep know your customer (KYC) requirement into the platforms – to enable *surveillance compliance* which – not least due to cost, and proliferation of personal data, will *not* be something they wish to undertake.

Such an obligation will also foster a hostile relationship between platforms and users, e.g.: forcing platforms to *actively prevent* use of superencryption tools like PGP and OTR which would undermine the backdoor.

This would create a strong obligation upon platforms to implement filtering, censorship and expensive hunting for illicit nuance and surreptitious meaning. The result will be stagnation.

False Positives: Privacy versus Safety

Not long ago I posted a tweet containing a snapshot from my home life:

> My 2yo nephew just demanded (& got) an e2e-encrypted WhatsApp bath-time singalong video call with his utterly beloved auntie; but all I could do is sit there and wonder what a mandatory "child protection" image classifier would make of the content, and to whom it would report it?
>
> Let's be utterly clear: there are a relatively tiny number [of] bad people in the world, who do bad things; but in an increasingly remote-living, remote-working society, touchpoints such as these keep families together. Yet the headlines are filled with Apps 'must check images for child abuse before publication'
>
> So: are call-centre workers, somewhere in the world, to be leaked copies of (literally billions of) private family moments, because a "bot" got triggered by what you said and what you did, on a video stream? If that ever happens, I'll be writing my own messenger software.

If my family is using the *field model* of an E2E app to enable a private and safe happy shared toddler's "bathtime funtime" – rubber ducks and all – something which could (and perhaps, should) be done by billions of people across the world, then what are we to make of calls for "automated reporting of child abuse" which this activity would almost certainly trigger?

Personally I think believe that – apart from breaking the *field model* and thereby breaking E2E – it would be massively illiberal, disproportionate and obscene for an app to speculatively and automatically leak nude pictures of my kids to *platform safety personnel*, invading my family privacy and speculatively turning those safety-personnel non-participants into voyeuristic statutory child-abusers.

"But it's for your child's safety" would not provide adequate justification. Tell it to the rubber duck.

A platform with such auto-reporting would be making and distributing CSAM where it did not exist before – and the victims would have no idea, possibly until the police knocked at the door, perhaps to investigate, or perhaps to say that their bathtime photos had been leaked by a rogue *platform safety* employee. This scenario has dreadful precedent [94] [95] and in the push for online safety, the problems of illiberality, privacy invasion, *false-positive*-handling, and quis custodiet ipsos custodes? all remain inadequately discussed.

Interoperability

Having *various things* work pleasantly in combination with *other things* is generally a great way to enable innovation and empower people. To assist in such empowerment, the EU has recently posted the Digital Markets Act which: [96]

- defines a set of conditions to identify a corporation as (what they call) a *gatekeeper,* alluding to the millions or billions of users who are "gated" up behind the platform's access controls – a place where they are unable to be accessed by *fourth party* startup companies who would otherwise enjoy the opportunity to monetise those users.

- once identified as a *gatekeeper,* the corporations must take steps to enable and permit fourth party startup companies to access "their" users, in order to enable innovation and open markets,

This all sounds great, what could possibly go wrong? [97]

What regulators believe they are doing

Regulators love to follow precedents, and there is a certain playbook in operation:

Breaking-up Ma Bell

The year is 1984: an American technology corporation has been abusing anti-competitive monopoly power. You are a crusading regulator who wants to improve consumer choice, empower innovation and open markets, and be seen as combating "vendor lock-in" and corporate dominance – possibly levying dramatic and politically useful huge fines in the process.

The corporation was Bell Telephone, the monopoly they abused was *provision of the local loop*, and the regulators were the US Department of Justice.

I've written about this at far greater length in *a blogpost*[98] which portended this report, but to summarise:

- it's expensive to lay supporting infrastructure and phone cables into someone's house, so it tends not to be done more than once, or at least not *casually*, especially in the 1970s and 1980s
- this naturally leads to a monopoly where the customer is forced to accept the services of the cable-laying phone provider, including any limitations and restrictions which may serve a larger and anti-competitive function
- *tradition* meant that local phone calls were provided for free, subsidised by big fees for calling long-distance or even calling a nearby town which happened to be in a different *area code*
- regulators decided to break up the expensive thing – long-distance calling – thereby leaving customers in the hands of their local (now smaller, but still) monopoly phone providers, with the additional fun of forcing them to navigate a maze of methods to call long distance… until technologies like Internet VOIP (e.g. Skype) and cellphones respectively disrupted the long-distance and local-provider models

Amongst the other lessons we can learn from this is that the benefits which the regulators claim to pursue are not necessarily ever going to be realised – or, possibly, doing so requires a paradigm shift such as *popular adoption of the internet* and *paying to move data rather than paying to merely speak to a person*; and that possibly all along the goal of regulation was to reduce the political power of [a huge corporation] which threatened to compete with the state for influence over peoples' lives.

Microsoft Word Format Wars

The year is 2000: an American technology corporation has been abusing anti-competitive monopoly power. You are (still) a crusading regulator who wants to improve consumer choice, empower innovation and open markets, and be seen as combating "vendor lock-in" and corporate dominance – possibly levying dramatic and politically useful huge fines in the process.

The corporation was Microsoft, the monopoly they abuse was *the undocumented and closed-source format of MS-Word ("Word") documents*, and the regulators were a hotch-potch of US-state, UK and EU Governments demanding *open standards.*

Anyone who has ever tried to import or export a natively-generated Word document into a word processor *other* than Word, knows that the results are a crapshoot: images in *slightly* different places, fonts that look *slightly* wrong – or in the worst case are missing – page breaks flowing differently… and this is the situation 10 to 20 years *after* solutions were first demanded and implemented.

What happened?

Microsoft dominance of the PC operating system space led directly to Microsoft's further dominance of the word processor application space, leading to preponderance of the proprietary Word `.DOC` file format and of organisations circulating draft `.DOC` files amongst themselves for purposes of editing and commentary – thereby creating not merely a network effect but also a commercial dragnet in which those organisations were effectively obliged to purchase huge numbers of Word licences merely in order to function.

From this observation it follows that proprietary document formats are a tool of monopoly; this did not go unobserved, for instance the states of Massachusetts, Texas, Minnesota, and California all considered or adopted legislation to adopt the OpenDocument format for word processor documents, popularised by *OpenOffice* [99] [100] [101] so that long-term government documents would not be hidebound to perpetual and backwards-compatible licensing obligations to Microsoft.

In the spirit of if you can't beat 'em, join 'em, after which you can embrace, extend, and extinguish 'em – Microsoft adopted ODF *and also* launched its *own* supposedly open and confusingly-named document format, `OOXML`, or Office Open XML:

> **Office documents:** In a memo to the Office product group in 1998, Bill Gates stated: "One thing we have got to change in our strategy – allowing Office documents to be rendered very well by other people's browsers is one of the most destructive things we could do to the company. We have to stop putting any effort into this and make sure that Office documents very well depends on PROPRIETARY *[Internet Explorer]* capabilities. Anything else is suicide for our platform. This is a case where Office has to avoid doing something to destory [sic] Windows."[102]

Contemporary analysis by the Free Software Foundation included:

> **What's wrong with Office Open XML?**
>
> Microsoft is attempting to block an established, free and open format by heavily pushing one they have much more control over, and they're using all their lobbying power to try and fast track it through the standards process. Unlike OpenDocument, which is well-supported and cross-platform, Microsoft's format is only supported by proprietary software from one vendor, and because it has been designed to implement every bug, glitch and historical feature from Microsoft's Office software, the specification to implement OOXML is over 6000 pages long, making it much harder for other software to implement the format.
>
> **Doesn't Microsoft software now support ODF?**
>
> More recently, Microsoft has added broken support for ODF to Microsoft Office. Open Malaysia and Family Holloway have more information on the problem. Microsoft has shown its true colors by working against the community, by trying to pretend they want to show support for a standard, whilst actively working to break ODF. To quote Slashdot: "Microsoft Office 2007 SP2 claims support for ODF, yet with hard work and careful thinking, they have successfully achieved technical compliance but zero interoperability!"[103]

… and further document format controversies played out in the UK, for instance regarding adoption of OOXML by the British Standards Institute.

After ten to fifteen years of this, people got bored. Rather than remain an abstract but vital constituency of victims to defend from corporate interests, archivists were left to solve their own problems using tools at their own disposal – typically `ODF` or `PDF` – and activists lost the will to fight even though the state of interoperability available to `OOXML` documents is suboptimal, uneven, and (overall) poor. [104] [105]

The lessons we can learn from this, include:

1. The benefits of data format interoperability are not as stupendous as advertised; some – perhaps most – most data *does not* have to *live forever*, and where it *does* then organisations with vested interest tend to make organisation-specific choices and solutions to address that challenge
2. Codicil: sometimes, perhaps often, organisations will make poor choices of format for data in which they are institutionally underinvested; but this is an organisational risk rather than a technical failure, and can/should be addressed through selective, needs-based, mandate of open standards
3. Any amount of passion regarding the essential nature and existential importance of *interoperability* will fade with both time and/or loss of lobbyist or academic funding.
4. For most people the practical extent and benefits of interoperability initiatives will be underwhelming when compared to the purported ones.

For Microsoft users: `OOXML` is probably familiar to you by the suffixes `.DOCX`, `.XLSX`, and `.PPTX`.

"Ivory Towers" and "Data Portability"

The year is 2008: American technology corporations have been abusing anti-competitive monopoly power. You continue to be a crusading regulator … *I think you know where this is going by now.*

The corporations are Google and Facebook – to name just two – and the monopoly they abuse is that people's data is *locked up* in *proprietary formats* in these *ivory-tower platforms* where users are *not able* to *make use* of *their own stuff*. The regulators were the European Union, although the platforms also used the debate to take holier-than-thou potshots at each other:

> Google recently added a caustic warning message when users attempt to export their Google Contacts to Facebook: **Hold on a second. Are you super sure you want to import your contact information for your friends into a service that won't let you get it out?** – BusinessInsider: The Interoperability of Social Networks, November 2010

Perhaps from the fallout of the word processor format wars, or perhaps because (in the heat of Web2.0) `XML` was still considered by some to be *sexy* – perhaps only surpassed by the even more cool and hipster-ish microformats – or perhaps because of early buzz which would eventually lead to GDPR the topic of data portability was very fashionable.

At this point I should declare a personal interest: I was part of a now-defunct open source project which sought to empower people by putting them in control of their data, allowing them to share it and monetise it as they saw fit; I moved in the same circles as several key proponents of Data Portability, and 14 years later I find it entirely unsurprising that the *Data Portability Vision & Mission* webpage will not load. [106]

Consulting instead the Internet Archive copy of the page, we learn:

> **Vision:** Data portability enables a borderless experience, where people can move easily between network services, reusing data they provide while controlling their privacy and respecting the privacy of others. [107]

… and a lot more besides. Data Portability was a vision that all data would be well-formed and well-specified, stored and shared in free and open formats, that a common understanding and ontology of those formats would be shared by all, and that nobody would deviate from these goals either from laziness, incompetence, fashion, or pursuit of competitive advantage.

What it did not answer terribly well was *a practical need* – for instance I would be able to download an XML archive of my Tweets from Twitter… and then, *what?* I could reuse, remix, or upload it to *what*, precisely? My Twitter tweets would not magically become emails by uploading them to Yahoo or GMail, and my downloaded Facebook status updates – shorn of wider Facebook-native contexts like *tagged friends* – would make for very poor blog entries if naively reuploaded to Wordpress.

This is not to suggest that the overall concepts were or are *useless* – it makes sense for people to be able to download their content from various platforms, not least for archival or other personal reasons. Google's Data Liberation Front did great work in this space, Facebook's Download Your Information similarly, both could always do more to help the user recover "value" that is lost by ripping the data away from its original context, but what we have is not too bad and gradually evolves to be better.

The arrival of the GDPR froze the thinking in this space, and this executive summary displays the regulator's wishful thinking: (my emphasis)

> **Article 20 of the GDPR creates a new right to data portability,** which is closely related to the right of access but differs from it in many ways. It allows for data subjects to **receive the personal data** that they have provided to a controller, in a **structured, commonly used and machine-readable format, and to transmit those data to another data controller.** The purpose of this new right is to empower the data subject and give him/her more control over the personal data concerning him or her.
>
> **Since it allows the direct transmission of personal data from one data controller to another,** the right to data portability is also **an important tool that will support the free flow of personal data in the EU and foster competition between controllers.** It will **facilitate switching between different service providers, and will therefore foster the development of new services** in the context of the digital single market strategy. [108]

Here we see the EU suggesting that Alice should be able to tell Platform2 to directly fetch all of her content from Platform1, to process and make it ready for her, all without her further intercession. This is not impossible – for comparison Open Banking does something very similar, but rests upon interoperation between heavily-underwritten companies in a very heavily regulated industry, sharing data of very limited scope and format.

Social networking is not a comparable industry, and the name Cambridge Analytica should quickly remind us all why proliferation and *the free flow of personal data … between controllers* is not necessarily an empowering experience for users.

This latter should not be a surprise: in 2012 Schneier linked to a white paper in the Maryland Law Review, raising points which are familiar, even sympathetic to the Digital Markets Act "gatekeeper" definition; some extracts from the introduction:

> We emphasize at the outset that the idea of data portability is appealing. As consumers, we like the convenience of easily moving all of "our" stuff to a new service if we so choose. […] More generally, data portability can address a "lock-in" or high switching costs problem – users start to use one service, such as Facebook, and then find it costly or technically difficult to shift to another service, even if they prefer the other service. […] concerns about lock-in and high switching costs have been extensively addressed in antitrust law. One crucial requirement in competition law is that market dominance must be shown, typically by demonstrating high market share […]
>
> Swire & Lagos; Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique

… but then we get to the areas of concern:

- […] poses serious risks to a long established E.U. fundamental right of data protection: the right to security of a person's data. Previous access requests by individuals were limited in scope and format. By contrast, when an individual's lifetime of data must be exported "without hindrance," one moment of identity fraud can turn into a lifetime breach of personal data.
- […] the second service is permitted to write interoperable code, despite objections by the first service. The new, mandated code must also perform at a high level of interoperability, transferring the data "without hindrance." In practice, achieving interoperability is often a difficult task, requiring tailored code to interact with different recipients. But the [Right to Data Portability] puts a new obligation on the first service to write the [Export/Import Module] and meet that ambitious standard."
- A key finding is that the [Right], designed to help consumers, appears to reduce consumer welfare as understood in competition law. Competition law, in both the U.S. and E.U., recognizes important efficiencies that can occur from lock-in for some situations; notably, a certain level of switching costs can encourage investment in new products and services, creating efficiency over time.
- With the absence of previous experimentation with data portability rules, and no consensus among experts about best practices, it is risky to lock in sweeping new requirements […] The general conclusion is that the [Right] deserves careful attention from academics and policymakers, both within the E.U. and elsewhere, and that a sweeping or badly implemented version of the [Right] could cause significant harm.

… and further down:

- The discussion here has presented three examples of as-yet undefined terms under [The Article]: "without hindrance", "structured and commonly used format[s]", and "other information provided by the data subject." Experience with [The Article] may reveal other textual challenges.

All of these challenges, and more, not to mention a poorly-founded understanding of E2E which excessively focuses upon delivery of end-to-end *encryption*, have comparable or identical challenges which afflict the Digital Markets Act's approach towards *messenger interoperability*.

The present day, the EU, and "messenger interoperability"

Today the corporations are "gatekeepers", and the monopoly that they abuse is *the network effect, a*Metcalfe's law, and the regulators are the European Union. The relevant law is the Digital Markets Act and it may or may not be too late to change this, but the foreseeable errors at stake should not go unremarked.

With this mental model we can see what likely captured the interests of regulators:

1. Messenger Applications are like phones – they connect people to enable them to communicate, and phones were a monopoly which needed regulating
2. Messenger Applications are like word processors – they exchange data in particular, often proprietary, formats and protocols, which are a common lever for monopolistic behaviour and need regulating with open standards
3. Messenger Applications are *ivory towers* – they lock-up users in a place where potential competitors cannot get at them, thereby excluding innovation and market growth; and it's hard for users to *leave* because of *"network effects"*
4. Further: Messenger Applications prevent people getting at the full value of *their* data, hampering access to that data by similarly locking it up inside the messaging apps
5. Therefore: the solution is to mandate interoperability

The problem with this analysis is that – from an E2E perspective – all of the supposed downsides which historically have demanded regulation are features (or are *consequences* of features) that you would rationally *desire* in an E2E solution.

This may be counterintuitive but before explaining I would first like to establish a small, shared understanding and vocabulary of…

Human communication

What are we doing as human beings, when we communicate? And how do we achieve it? I'd propose[109] something which:

- … starts with a *meaning* (or a *concept*, *idea*, *emotion*, or *request*, etc) that one person wishes to share with another
- This person has one or more *languages* at their disposal, where a *language* is a combination of *lexicon* and *grammar*
- A *lexicon* is a set of *words* which are *tokens* which represent *objects* or other *concepts* – including some *concepts* which exist to support *grammar*…
- … and where *grammar* rapidly decomposes into several things but primarily:
- *Syntax* is a shared set of rules regarding how to properly compose and order words in order to convey *meaning*, and…
- *Morphology* describes (amongst other things) how to inflect multiple words in their syntactic ordering in order to convey further concepts; this rapidly leads to *accents* and *punctuation* and so forth, all of which are large subjects in themselves
- Aside: a *vocabulary* is that portion of a *lexicon* which a person has at their own disposal
- Also there is the useful concept of phatic communication, where words convey "metadata" (or "meta-meaning?") for initiating or maintaining a line of communication, or for soliciting or eliciting further words within that line of communication
- Where we – in the English language, at least – then go wrong is how we talk about what happens next: we use the word *medium* to describe *expression* of language: the medium of *speech*, the medium of *text*, the medium of *dance*. But…
- … we also conflate *media* with what I prefer to call *transport*; we talk about the *transport media* of *print and video and 'digital'* whilst previously using the same noun to describe *expressive media of speech and text and dance and imagery*. Software engineers call this a *layering violation* and I believe that the confusion caused by conflation of *transport* and *expression* leads to the most critical misunderstandings of digital communication which we observe in this space

Why distinguish expressive- vs: transport media?

The word telecommunication literally means *communication over a distance*, and with that same prefix we also get:

- telegraph, or *writing over a distance*
- telephone, or *sound over a distance*
- television, or *sight over a distance*

These *transport media* have become of incalculable value for modern peoples to share *concepts* and *meanings* by various expressive media – including, as a slightly extreme example, digital video of a dance, where we use numbers to communicate meaningful and graceful movement of people.

Prior to the Internet the primary means of person-to-person *communication at a distance* was the *telephone*, and Alice would speak *speech* into a microphone which *transported* a muted and filtered representation of the audio from Alice's phone, over wires and (Almon Strowger's) switches to Bob's phone, where Alice's voice would be reproduced to Bob through a small speaker; and vice-versa in the opposite direction.

The boundaries of the telephony user experience are (conceptually) quite small: a box or widget with numbers 0 through 9 and a few other buttons, some long wires or their modern equivalents, a microphone and a speaker. Internally there are some network-performance features such as filtering audio down to a narrow frequency range in order to permit more effective use of old transport wiring, but these features are not under the control of the user.

But: with a phone all matters of expression: language, lexicon, grammar, syntax, voice, tone, phatic communication (etc) are *wholly* the responsibility of Alice and Bob, and there is negligible *linkage* between the telephone and the user. The phone is a "dumb box", Alice speaks into one hole, Bob listens at another, and vice-versa. Alice and Bob might be speaking English, Swahili, or Esperanto, all without care or consequence to the overall telephone system.

Telephones are *transport media* – communication-enabling hardware similar to others which governments have in the past regulated: fax machines, radio transmitters, printing presses, etc.

Governments tend to feel confident about regulating transport media.

E2E apps are expressive media

Here is what the Digital Markets Act has to say about messenger software, including "end-to-end encrypted" messenger software:

> … on contestable and fair markets in the digital sector (Digital Markets Act)
>
> Article 7 […]
>
> 1. […] The gatekeeper shall make at least the following basic functionalities referred to in paragraph 1 interoperable where the gatekeeper itself provides those functionalities to its own end users: (a) following the listing in the designation decision pursuant to Article 3(9): (i) end-to-end *text messaging* between two individual end users; (ii) sharing of *images*, *voice messages*, *videos and other attached files* in end-to-end communication between two individual end users … within 4 years from the designation: (i) end-to-end *voice calls* […]

2. *[there is no section 2?]*
3. The level of security, including the end-to-end encryption, where applicable, that the gatekeeper provides to its own end users shall be preserved across the interoperable services.
4. The gatekeeper shall publish a reference offer laying down the technical details and general terms and conditions of interoperability with its number-independent interpersonal communications services, including the necessary details on the level of security and end-to-end encryption. The gatekeeper shall publish that reference offer within the period laid down in Article 3(10) and update it where necessary.
5. Following the publication of the reference offer pursuant paragraph 3, any provider of number-independent interpersonal communications services offering or intending to offer such services in the Union may request interoperability with the number-independent interpersonal communications services provided by the gatekeeper. Such a request may cover some or all of the basic functionalities listed in paragraph 2. The gatekeeper shall comply with any reasonable request for interoperability within 3 months after receiving that request by rendering the requested basic functionalities operational.
6. The Commission may, exceptionally, upon a reasoned request by the gatekeeper, extend the time limits for compliance under paragraph 2 or 5 where the gatekeeper demonstrates that this is necessary to ensure effective interoperability and to maintain the necessary level of security, including end-to-end encryption, where applicable.
7. The end users of the number-independent interpersonal communications services of the gatekeeper and of the requesting provider of number-independent interpersonal communications services shall remain free to decide whether to make use of the interoperable basic functionalities that may be provided by the gatekeeper pursuant to paragraph 1.

Problems and concerns are numerous – very like the GDPR issues raised in Swire & Lagos (q.v.) and unlike the report you are reading:

- The Act specifies no definition for *end-to-end encryption* nor what it means for end-to-end encryption to be, or not be, *preserved?*
- Also, what is a *level* of security, and how does that impact the presumed requirement for end-to-endness? Is a *level* maintainable by breaking E2E and interposing a man in the middle with encryption of equal key length?
- The Act refers to *effective interoperability* and without definition of what *effective* means and who decides that matter?
- Worryingly, the Act further refers to *necessary levels of security* without definition of what *necessary* means and who decides *that* matter, and what would happen if they decided that the demands of security were somehow *excessive?*
- The Act is written from a perspective focused purely on *function* – text-messaging, images, videos, attached files, group chats, voice calls – as opposed to *user-value* and *user-experience* such as:

    1. assurance of data-storage privacy amongst all participants, e.g. *"Signal doesn't do backups without encryption"*
    2. automated data destruction, e.g. *disappearing messages* in Messenger, Signal and WhatsApp, *disappearing images* in Snapchat
    3. mutually agreed participant behavioural management and monitoring, e.g. *screenshot detection* in Snapchat and Messenger
    4. sending what *kinds* of images, what *emojis*, what *gifs* – and do they count as *images* or *attached files*, or as something else entirely?

Over the past 20 years we have moved from a world where it is novel to be able to share a text message or image at all to one where semantic agency – the intentional, emotional and privacy-management aspects of communication – all have equal standing. We send GIFs because they offer a quick means to express meaning which otherwise might take a thousand words. We use disappearing messages because to not do so might lead to arrest.

With this understanding would the regulator demand that all interoperable applications *also* implement *those* features, or might they finally accept that different apps make different value propositions which extend beyond *moving data around* into *how that data is managed* and *what it is meant to convey*.

Apps are not simple, interoperable, fundamentally-identical telephones; instead they are helpers to enable us to speak clearly and privately when standing in a field of wires.

GIFs and *Emoji* hugely expand our lexicon. Personalised *stickers* and *reactions* provide better phatic cues. [110] Each app internally provides morphology and syntax structures to better transport these expressions for us. Messaging apps are *expressive media*, and – like the opposite of a pidgin – each of these apps embiggens our native language(s) in different ways that make them more fit for online expression. We benefit from having *more difference* and *more diversity* of approach in this embiggening – in how apps are engineered to help us *express* ourselves better, so that there is evolution and improvement.

We need more and different and diverse apps, not fewer and more standardised. Demanding "a single inbox" shuns this change. The state calling for "interoperability" above all else – in order to enable "open markets" of startup access to cattle-like users – will not deliver, and indeed will even *hamper*, evolution of the improvements that we need.

Regulators – following their usual playbook – believe that apps are fungible, technological, monopolistic transport media, deserving of regulation; but in that pursuit they are heavily impinging upon, even chilling, the newest form of expression that is available to us.

With this understanding we can revisit the "ivory towers and telephones" thinking which likely misled regulators into demanding interoperability in the first place:

- Messenger applications *do* enable communication between arbitrary numbers, even billions of people; but those people are not locked into a single app by means of some physical scarcity like a "cable" – apps are abundant, and there is (or should be) nothing anticompetitive to prevent their coexistence on the same phone
- Whether the message formats that apps exchange amongst themselves are "open" is not relevant – they can be open, but they don't have to be – because internal data formats are not relevant to service provision and user experience; also: deciding, publishing, and managing life cycles for data formats which don't need to be public, is onerous, time-expensive, and brakes development
- Network effects create huge billion-person communities who can all intercommunicate securely with E2E. As a user you want a few of those to exist. Nothing prevents a person from using several messenger apps to address different communities, often for different purposes. Those who express a vital need for *"single inbox" solutions* to messaging reflect the legacy view of messengers as transport, rather than expressive, media. They see messengers as *a different kind of email.*
- Personal Opinion: one of the funny things about network effects is how they are generally presented as making it hard or impossible to "leave" a platform, until it turns out that that's not true: 2021: Why Millions of People Are Leaving WhatsApp, and Downloading Signal and Telegram Instead
- In the *field model* someone who wishes to "leave" a platform is proposing either to break-off all communication and walk out of the field entirely, or else they want to drag themselves and all other participants into another field (i.e. another app, for instance "move everyone from WhatsApp to

Signal"). Any "interoperability" solution means standing in another field and shouting across the fence to everyone else who is still standing in the first one

- *Aside:* The solution to (e.g) iMessage not being available on Android – if that is really an anticompetitive concern – is to demand that Apple produce an iMessage client for Android, rather than that Apple open up APIs and break E2E guarantees in the hope that a secure and usable fourth party Android client will be created by… somebody.
- For guarantees of E2E the users want only the best and latest code to be in operation, and for the provider to be invested in delivery of the best solution; so you have to permit them a degree of lock-in (*"a certain level of switching costs can encourage investment in new products and services"*) and freedom to curate and restrict access by tools which do not properly and fully utilise the communications space that is provided (i.e. *"the field"*)
- The fundamental goal of an E2E messenger is to lock-up data where nobody else can get at it, not even the third party / platform; the participants become responsible for managing and sharing your data, you have the agency and authority. To suggest that providing this facility is part of a broader platform goal to prevent data sharing is to misapprehend the designed intent of enabling private communication.

Activist perception and disagreement…

A recent blogpost by Simon Phipps – a noted proponent of open source and open document formats – makes for relevant reading:

> **Interoperability Depends On The Use Case**
>
> When I was working on a paper on interoperability mandates [111] for The Internet Society, early reviewers complained that some sections seemed to imply only 100% functional equivalence and interoperability would be acceptable, and told us "much smaller percentages are perfectly adequate." So how much interoperability is enough interoperability? The answer, dear to the hearts of every politician, is "it depends."

I encourage you to read the whole blogpost, but to quote two key points:

> **Document Interoperability:** […] Given the near impossibility of delivering a user experience perceived as identical [to MS-Word] on alternative implementations, how has software like Google Docs been able to gain such a large user base? Instead of a focus of a substitutable user experience, Google started with a compelling new capability – real-time user collaboration and change tracking – and implemented good-enough interoperability using open source tools. [112]

… and:

> **Messaging Interoperability:** […] For some users, the only function that matters is sending a short, text-only message to another person and having the text faithfully reproduced. [… yet, another…] user needs to be sure the message they are sending is visible only to its recipient so needs not just the text exchanged but reliable and secure encryption using private keys accessible only to their owners but working fully on the systems at both ends. To them the transmission of the text would be an error if the end-to-end integrity and repudiability of the conversation were not guaranteed.
>
> Again, the same systems may have use-cases with wildly different needs for interoperable

> functionality. Broad statements about "all-or-nothing" or "just the basics" serve the discussion poorly. [113]

This report deals only in E2E which (to recap) we define as *end-to-end secure and encrypted communication*; the text of the Digital Markets Act aside, [114] there is no such objective thing as a *level of security*; instead each E2E application provides a solution to a *functional requirement*, in the process mitigating *risk* from *threat actors* within a given *threat model*.

A concrete (and partial) example of this would be:

- application: Snapchat
- functional requirement: sharing pictures of you and your friends out when clubbing and having fun
- threat model: non-participants seeing embarrassing, even compromising pictures of you all having fun
- threat actors: parents, employers with privileged access to work phones
- risk mitigations: shared pictures are ephemeral, viewable once-only, hard to screenshot, not saved to device storage, not backed-up, end-to-end encrypted

Exactly as Simon notes, some will see [Snapchat] as just another short, text-only messaging platform; however if that is the defined "level" of "interoperability" which needs to be met then it is *very poor interoperability,* because – irrespective of the DMA – basic *text messaging,* or even basic *image messaging,* does *not* reflect the functional requirement for Snapchat.

To be more blunt than Simon: from the perspective of delivering E2E it is the trio of *functional requirement*, *threat model*, and *risk mitigations*, which define the metric for the "level of security" that the app provides. Any fourth party *alternative client*, if not actually maliciously intended, must meet or exceed that "level of security" otherwise it is trading-down part of the E2E application value proposition and user security in order to attract potential users.

For the purposes of E2E, 100% interoperability [115] really is obligatory to even be *adequate* – in which case you might just as well use "the real thing" rather than some fourth-party competitor.

Also there's the open political question of fourth party intent versus impact:

> [… what if] WhatsApp is forced to "open up APIs", and Telegram decides to implement a "interoperable" client as part of Telegram; and then Telegram starts aggressively upselling itself to move (e.g.) Iranian activists out of end-to-end encrypted Signal-protocol WhatsApp chats, into Telegram ones.
>
> Breaking Up "Ma Zuck"

… what should our considerations be, where interoperability for any motive whatsoever, exposes vulnerable groups to hitherto nonexistent risks? i.e. The Snappening, but with dissidents, interception, rubber hoses, and torture.

Gatekeeping the Gatekeepers

Proponents of interoperability are split regarding what outcomes they want from the project; some of them are clearly focusing on it as a means for regulators to *rein in* big corporate power:

> An interoperability requirement for large online platforms has been suggested by the European Commission as one ex ante (up-front rule) mechanism in its proposed Digital

> Markets Act (DMA), as a way to encourage competition. The policy goal is to increase choice and quality for users, and the ability of competitors to succeed with better services. The [rule's] **application would be to the largest online platforms, such as Facebook (social media and instant messaging), Google (search and Android), Amazon (marketplace), Apple (iOS), and operating system ancillary services, such as payment and app stores.** Interoperability as a tool for competition regulation

…and we can see reinforcement of that position in Dr Ian Brown's – the author's – tweets confirming that "small" messenger services like Signal would not be classed as a gatekeeper and would be exempt from interoperability demands:

> If you read the final DMA interoperability obligation, you will see that neither nor Signal or Telegram are affected in any way. They are not "gatekeepers" in the DMA sense (you will have to look up those definitions in earlier versions; I don't have the final text)[116]

But then we contrast that with the *vision* of other proponents:

> What matters most for users is that the DMA mandates interoperability between messaging services. **For instance, if you are a WhatsApp user, the DMA says that you should be able to message someone on Signal.** Many security experts have expressed concern that doing so may risk dropping end-to-end encryption. **We disagree.** The language in the final text clearly states that gatekeepers should make their services interoperable only if end-to-end encryption can be maintained throughout the communication services.
>
> [117]

This report has already dealt with the glibness and wrongness of *"we disagree"*, but it's worthwhile wondering: in the long term, whose vision will win? Will interoperability regulation continue to *only* be targeted at the biggest of corporate messenger networks? Or will the EU – or even more zealous nations, like California – attempt to mandate interoperability for any network with (say) more than a mere 1 million users?

And is it not a chilling effect upon innovation to legislate that new platforms are free to build their own hyper-secure and richly functional "ivory tower" or "walled garden" applications… *however* if their applications ever become sufficiently popular by dint of that security and function, those platforms will become obliged to drill holes in, or otherwise dismantle, the very features which helped make them a success?

'Monopoly' as leverage against state overreach

Aside: whilst I am busy committing heresy against several core beliefs of digital rights civil society – open source, open formats, metadata is sacrosanct, making a profit is wicked, corporations are evil – let's throw another one into the mix:

walled-garden 'monopolies' are an effective buttress against state surveillance

At the moment – with the possible exception of iMessage in China – all the big-platform GAFAM and related social media platforms operate on a "take it or leave it" basis. Generally there is one application, it is deployed to a target market – usually globally – and any per-country-vertical differentiation is handled by the app itself.

Without interoperability there is little scope for alternative clients, especially in the face of security controls exerted by the Google and Apple App Stores; and there is little desire by smaller repressive regimes to (e.g.) ban access to WhatsApp in their country, as to do so would foment revolt.

However: with the possibility of interoperability comes new opportunities for oppression; there would be nothing to stop (e.g.) Turkey from creating its own, surveillance-enabled client (NedirApp? WhatsTurk?) and then *banning the official WhatsApp client* from being available to Turkish users of the Google and Apple App Stores.

Security nihilists may complain that "… yes but Google and Facebook can already spy on you on behalf of all those governments anyway, so they can already do that…" – however that's misrepresentation; aside from several other reasons the challenge of *surveillance compliance* (q.v.) makes it infeasible for platforms to surveil on behalf of many countries other than the United States… which for many people living in repressive regimes is an entirely acceptable threat model.

So: interoperability strengthens state influence over the upstarts of technology companies. That includes all states. That impacts all peoples. It's a matter for concern.

Remembering the Past

People writing more than 10 years ago:

> A similar network interoperability battle happened last decade [viz: 2000-2010] among Instant Messaging networks. **AIM was the dominant network for many years and refused to interoperate with other networks. Google Chat adopted open standards (Jabber) and MSN and Yahoo were much more open to interoperating. Eventually this battle ended in a whimper – AIM never generated much revenue, and capitulated to aggregators and openness.** (Capitulating was probably a big mistake – they had the opportunity to be as financially successful as Skype or Tencent).
>
> November 2010: Chris Dixon: The interoperability of social networks

… and…

> From the beginning, we designed Google Talk using open standards so that you could connect to your friends and family using any chat product, making communication as easy as possible. A few years ago, we announced our partnership with AOL which made it possible for people to chat with AIM users right from inside Gmail. Today, we're happy to report that AOL has now made it possible to chat with AOL contacts across a variety of Google services: not just Gmail, but also iGoogle, Orkut, and Google Talk on Android phones. […]
>
> May 2011: Official Gmail Blog

Today:

- AIM (AOL Instant Messenger) is dead
- Google Chat is dead
- MSN Messenger is dead
- Yahoo Messenger is dead
- Skype is alive, although gradually being deprecated in favour of MS-Teams
- Tencent QQ is very much alive
- Few if any XMPP-based solutions (was: Jabber) remain interoperable, not least because of the widespread use of *extensions*

Conclusion: *Interoperability* doesn't power the success of messaging products.

Instead, solving problems for the user, with great design, reliable execution, rich featureset, simple operation, and low-to-zero user cost, along with serious, long-term commitment from the platform [118] [119] – help messaging products succeed.

Summary of Interoperability and the Field Model

Alice walks into a field. Bob walks into the field next door and shouts *"… this will be fine, don't worry about it"* and over the fence he throws one end of a long hosepipe and a plastic funnel to Alice. Carol is in a third and more distant field and asks everyone to shout a bit louder…

Interoperability does not make it impossible to have E2E communication, but it does introduce a lot more complication, a lot more risk, makes it harder for the participants to see and detect eavesdroppers, and reduces certainty regarding who or what helpers the participants have brought into the field with them.

Interoperability does not inherently break the *field model* but it does *seriously compromise* the trustworthiness of E2E which is offered – all the more perversely – by the *largest* of platforms, or by any platform which has the eventual misfortune to become large.

Afterword

Civil society discussion of E2E often becomes bogged down in apparent complexity, and that this state of affairs continues is greatly to the advantage of those who want to retain surveillance capability over E2E.

I believe that a lot of this complexity simply vanishes with a fuller understanding of what E2E achieves – and where its boundaries are – which enables better discourse.

Attempting to summarise everything above, a few final thoughts:

- Whether the *field model* constitutes a "natural right" (or some other arbitrary label) does not really interest me; but even today you and your partner can put down your phones, walk into a field away from eavesdroppers, and have a private conversation. Regrettably, you will now have to keep an eye out for drones, sweep the area for microphones, and keep your voices down. Perhaps you could carry a white-noise generator to assist your privacy, very much as encryption provides for private, digital messaging.
- E2E implements the *field model* for digital communication, where participants are separated by distance and must communicate amongst themselves over networks. The law seems content to permit private speech amongst consenting parties in physical fields, and therefore it seems extraordinary to consider it an exceptional risk in digital ones. Possibly the state has become addicted to the concept of wiretaps?
- The *fundamental questions* from the foreword are most urgent: in a physical or a digital field, participants are able to share secrets amongst themselves. Should individuals remain free to keep a secret, even from the state? Should consenting parties remain free to communicate in a manner that is private, even from the state? What arbitrary metric makes this capability *too much* or *too dangerous* to be acceptable to society?
- And the third fundamental question: should third parties ever be obliged to *not enable* – or even *actively prevent* – access to the above freedoms?
- We now understand that to *actively prevent* E2E would require platforms to continuously monitor *all* speech to ensure that participants are not surreptitiously exchanging encryption keys amongst themselves. *Inhibiting user privacy requires eternal vigilance.*

- Per the *field model*: E2E with a "backdoor" is *not* E2E at all; so the choices for a platform facing state hostility towards E2E deployment are either to be brave and implement E2E in the face of political opposition, or to be cowardly and build something which does not satisfy the *field model*, risks leaks of user data, and will eventually expire by being less security-competitive than open source distributed E2E communications tools. In the spirit of accelerationism some civil society technologists would welcome trying to bring about this (potential) eventuality – e.g. the 'fall of Facebook' – but without E2E a lot of innocent people are going to suffer in the meantime (if it ever happens at all) and initiatives like *interoperability* will perversely only sediment extant providers rather than supersede them. Perhaps our radicalism should focus upon innovation rather than upon control?

… and what can civil society do?

- Pursue *end-to-end secure and encrypted communication that is free from (mechanisms that enable) general surveillance*, noting that actual *encryption* is merely one small part of that promise.
- Refine understanding of the boundaries of E2E, and with this make a clear decision whether (or not) platforms should be free to use metadata to provide both user safety and funding/revenue/profit
- If they should *not* be free to use metadata, explain why is it necessary to *stop them* rather than to *create and popularise* alternative platforms which offer a *different balance* of metadata privacy, user safety, performance, robustness, and funding/revenue/profit?
- And *re:* that *different balance*: consider, discuss and explain what would be the impact upon two or three billion ordinary – and mostly non-technical – people, of moving to "alternative" platforms? Provision of Safety? Abuse prevention? Reliability? Ability to scale? Freedom from local state influence? Exposing cross-border communications to *multiple* sets of state surveillance? Must the big platforms [120] be brought down in order to foment change? How might oppressive regimes [121] leverage the proportionately greater influence that they would have over multiple small, distributed, even *federated* platforms? [122] Would the people be better served by having a greater *diversity of E2E providers* rather than a lesser number of providers but with *interoperable clients*? Including or excluding the big ones?
- Further: having decided and explained their positions on all of the above, civil society should also observe, compare, and judge platforms on the transparency of their offerings regarding what metadata is/is-not available to them, [123] [124] how they use it, how and when they dispose of it, and for what purposes it is used and by whom – in the meantime?

This latter is a long list of questions which need to be brought into the public debate, and for civil society's position to be credible they must be considered, argued, and explained with the same level of transparency and to the same depth that we demand from platforms, in order to know how much we should trust their offerings of E2E.

Thanks

I would like to thank:

- Caroline Wilson-Palow
- Ed Geraghty
- Priya Dutta
- Runa Sandvik
- Simon Phipps
- Susan Landau

… for their generosity, kind assistance and commentary in the preparation of this report.

Footnotes

1. *Old Bailey Solicitors, Being Served With a S49 RIPA Notice*: https://www.oblaw.co.uk/being-served-with-a-s49-ripa-notice/ [return]
2. *Kerr, The Law of Compelled Decryption is a Mess: A Dialogue*: https://reason.com/volokh/2020/08/10/the-law-of-compelled-decryption-is-a-mess-a-dialogue/ [return]
3. *Diffie & Landau, Privacy on the Line, Introduction*: "But before the electronic era conversing in complete privacy required neither special equipment nor advanced planning. Walking a short distance away from other people and looking around to be sure that no one was hiding nearby was sufficient. Before tape recorders, parabolic microphones, and laser interferometers, it was not possible to intercept a conversation held out of sight and earshot of other people." [return]
4. *Froomkin, The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*: "Under current law, a person communicating via new media is less able to ensure her privacy than were speakers in the late eighteenth century. If Thomas Jefferson wanted to speak privately to John Adams, they could go for a walk in an open field where they could see any potential eavesdroppers from a mile away." [return]
5. *Froomkin, q.v.*: "At the time Americans adopted the Bill of Rights, private communications were far more secure than they are today. Before the invention of the telephone, the radio, and the long-distance microphone, one could have a secure conversation by going for a quiet walk in an open field. Correspondents could encrypt letters in ciphers that no government could break." [return]
6. *Fraser, Virginia Journal of Law and Technology; The Use of Encrypted, Coded and Secret Communications is an "Ancient Liberty" Protected by the United States Constitution*, throughout [return]
7. *Source: Wikipedia*: https://en.wikipedia.org/wiki/Postal_censorship#Pre-World_War_I [return]
8. *See also: National Archives*: https://discovery.nationalarchives.gov.uk/details/r/C5759 [return]
9. *Wikipedia: Strowger Switch*: https://en.wikipedia.org/wiki/Strowger_switch#History [return]
10. *Investigatory Powers Act 2016* s20.2c & s20.4: "Grounds on which warrants may be issued by Secretary of State… if it is necessary… in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security… only if the information which it is considered necessary to obtain is information relating to the acts or intentions of persons outside the British Islands" https://www.legislation.gov.uk/ukpga/2016/25/part/2 [return]
11. including people who have *left* a group chat of which they were previously a participant [return]
12. reducing opportunity for data theft, providing a universal and secure foundation for business communications innovation, etc.!: [return]
13. *Wikipedia: Babington_Plot*: https://en.wikipedia.org/wiki/Babington_Plot#Infiltration [return]
14. *Wikipedia: pneumatic tubes*: https://en.wikipedia.org/wiki/Pneumatic_tube [return]
15. *Wikipedia: The Internet is a series of tubes*: https://en.wikipedia.org/wiki/Series_of_tubes [return]
16. With the advent of high-bandwidth and low-latency cryptography the use of physical armouring for network cable has diminished, however an online search for: `ethernet "pressurized conduit"` will reveal historical examples [return]
17. *formula:* `(n*(n-1))/2`: https://math.stackexchange.com/questions/17747/why-a-complete-graph-has-fracnn-12-edges [return]
18. proviso: assuming that their devices are not compromised by unwanted fourth parties; see "TCB," below [return]
19. Doubtless this will surprise some legal theorists. Certainly it has surprised at least one QC. [return]
20. *To the UK: An Encrypted System That Detects Content Isn't End-to-End Encrypted*: https://cdt.org/insights/to-the-uk-an-encrypted-system-that-detects-content-isnt-end-to-end-encrypted/ [return]

21. *Alex Davies-Jones, Shadow Minister DCMS, Online Safety Bill Debate, 9 June 2022* – "It is a false argument made by those who believe that impacting end-to-end encryption will limit people's privacy. The technology does exist … able to scan without preventing the encryption of the data. It simply scans for those images and transfers them over existing databases. It would have no impact on anybody's right to privacy…" https://www.theyworkforyou.com/pbc/2022-23/Online_Safety_Bill/08-0_2022-06-09a.326.9#g337.2 [return]
22. *We're not talking about weakening encryption or defeating the end-to-end nature of the service*: https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate [return]
23. *Grammarly*: "Can anyone at Grammarly read my text? No, only those who have an approved need to access certain data are given access to that data-access is granted via specific, audited permissions, and access to data requires review and approval by the responsible managers." https://support.grammarly.com/hc/en-us/articles/360003835331-Can-anyone-at-Grammarly-read-my-text [return]
24. *Grammarly*: "… restricts employee access to customer data across our network, infrastructure, and services. Only those authorized to access data critical to their work may do so." https://www.grammarly.com/trust#control-access-to-data [return]
25. There *is* an edge case where Alice *can* prove to the other participants what software she is running, but this presumes use of an overarching trust model which impacts her autonomy; see discussion in *MDM*, below [return]
26. *Timing Attacks in Low-Latency Mix Systems*: https://www.freehaven.net/anonbib/cache/timing-fc2004.pdf [return]
27. *Browser-Based Attacks on Tor*: https://www.mit.edu/~ecprice/papers/tor.pdf [return]
28. *DeepCorr: Strong Flow Correlation Attacks on Tor Using Deep Learning*: https://dl.acm.org/doi/10.1145/3243734.3243824 [return]
29. *DeepCorr q.v., YouTube*: https://www.youtube.com/watch?v=_OKLtKgEn4k [return]
30. *Speculative Tor Attacks*: https://www.whonix.org/wiki/Speculative_Tor_Attacks [return]
31. *Your Threat Model is Not My Threat Model*: http://blog.totallynotmalware.net/?p=53 [return]
32. Compare *Cui bono?*, Who benefits? [return]
33. To avoid 'compliance with (surveillance) local laws and regulations' being considered 'value' [return]
34. for non-lawyer: potentially criminal intention [return]
35. for non-lawyers: potentially criminal action [return]
36. for lawyers: this may be different to how you normally consider law relating to data collection and compatible purposes; if so, enjoy. [return]
37. For the avoidance of doubt: From my experience pretty much every "bad" thing that everyone assumes happens, *has* been tried by every platform at least once. By and large the results have been uniformly dreadful and pointless, otherwise the techniques would be formalised into an industry standard with annual conferences, etc.… [return]
38. i.e. monetise against [return]
39. e.g. Facebook 2017 revenue USD 41bn, userbase 2bn, mean revenue per user = USD 21; i.e. less than two dollars per user per month https://twitter.com/AlecMuffett/status/1016321180117209088 [return]
40. *e.g. Snapchat, where text messages are not E2E*: https://snap.com/en-GB/privacy/privacy-by-product [return]
41. *Facebook Messenger: The battle over end-to-end encryption*: https://www.bbc.co.uk/news/technology-60055270 [return]
42. *Revealed: UK Gov't Plans Publicity Blitz to Undermine Privacy of Your Chats*: https://www.rollingstone.com/culture/culture-news/revealed-uk-government-publicity-blitz-to-undermine-priva [return]
43. including fourth party 'RED' demands for otherwise 'AMBER' metadata collection [return]
44. *Compare: marginalisation of ITU-T protocols such as X.25, except in the service of the more freewheeling TCP/IP*: https://en.wikipedia.org/wiki/X.25 [return]

45. i.e. the cryptographic technology, as distinct from our applied definition of E2E as 'end-to-end secure and encrypted communication' [return]
46. Certainly it beats the hell out of trying to manage your PGP 'private key' [return]
47. … and yet even then still contentious [return]
48. … rather than via an intentional, although possibly unrealised/unknowing, "leak" from a participant [return]
49. *See also: Wikipedia: Computational indistinguishability*: https://en.wikipedia.org/wiki/Computational_indistinguishability [return]
50. *See also: Wikipedia: Distinguishing attack*: https://en.wikipedia.org/wiki/Distinguishing_attack [return]
51. *See also: Wikipedia: Ciphertext indistinguishability*: https://en.wikipedia.org/wiki/Ciphertext_indistinguishability [return]
52. *EPIC Archive*: https://archive.epic.org/crypto/legislation/freeh_797.html [return]
53. *India proposes alpha-numeric hash to track WhatsApp*: https://economictimes.indiatimes.com/tech/technology/govt-proposes-alpha-numeric-hash-to-track-whatsapp-c [return]
54. *New Intermediary Rules in India Imperil Free Expression, Privacy and Security*: https://cdt.org/insights/part-2-new-intermediary-rules-in-india-imperil-free-expression-privacy-and-security/ [return]
55. *Hash constant: Govt's solution to tracing originator of viral messages*: https://www.hindustantimes.com/india-news/hash-constant-govt-s-solution-to-tracing-originator-of-viral-mess [return]
56. *Principles for a More Informed Exceptional Access Debate*: https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate [return]
57. *On Ghost Users and Messaging Backdoors*: https://blog.cryptographyengineering.com/2018/12/17/on-ghost-users-and-messaging-backdoors/ [return]
58. *An Open Letter Against Apple's Privacy-Invasive Content Scanning Technology*: https://appleprivacyletter.com/ [return]
59. *Apple's Plan to "Think Different" About Encryption Opens a Backdoor to Your Private Life*: https://www.eff.org/deeplinks/2021/08/apples-plan-think-different-about-encryption-opens-backdoor-your-priv [return]
60. *Bugs in our Pockets: The Risks of Client-Side Scanning*: https://www.cs.columbia.edu/~smb/papers/bugs21.pdf [return]
61. *Apple responds to critics of CSAM scan plan with FAQs…*: https://www.theregister.com/2021/08/09/apple_csam_faq/ [return]
62. *Apple quietly deletes details of derided CSAM scanning tech from its Child Safety page without explanation*: https://www.theregister.com/2021/12/16/apple_deletes_csam_scanning_plan/ [return]
63. *Preventing Child Exploitation on Our Apps*: https://about.fb.com/news/2021/02/preventing-child-exploitation-on-our-apps/ [return]
64. *Understanding the intentions of Child Sexual Abuse Material (CSAM) sharers*: https://research.facebook.com/blog/2021/02/understanding-the-intentions-of-child-sexual-abuse-material-csam [return]
65. *Well, this is some interesting reading for the afternoon*: https://twitter.com/AlecMuffett/status/1524066299600683008 [return]
66. *Question for @YlvaJohansson…*: https://twitter.com/AlecMuffett/status/1525741695010217987 [return]
67. *Copyright Filters Are On a Collision Course With EU Data Privacy Rules*: https://www.eff.org/deeplinks/2020/02/upload-filters-are-odds-gdpr [return]
68. *The EU's Copyright Directive Is Still About Filters, But EU's Top Court Limits Its Use*: https://www.eff.org/deeplinks/2022/05/eus-copyright-directive-still-about-filters-eus-top-court-limits-its-use [return]
69. *WeChat Surveillance Explained*: https://citizenlab.ca/2020/05/wechat-surveillance-explained/ [return]

70. *How WeChat uses one censorship policy in China and another internationally*: https://citizenlab.ca/2016/11/wechat-china-censorship-one-app-two-systems/ [return]
71. *Mutually Assured Surveillance*: https://alecmuffett.com/article/15393 [return]
72. *Timing Attacks in Low-Latency Mix Systems*: https://www.freehaven.net/anonbib/cache/timing-fc2004.pdf [return]
73. *Browser-Based Attacks on Tor*: https://www.mit.edu/~ecprice/papers/tor.pdf [return]
74. *DeepCorr: Strong Flow Correlation Attacks on Tor Using Deep Learning*: https://dl.acm.org/doi/10.1145/3243734.3243824 [return]
75. *DeepCorr q.v., YouTube*: https://www.youtube.com/watch?v=_OKLtKgEn4k [return]
76. *Speculative Tor Attacks*: https://www.whonix.org/wiki/Speculative_Tor_Attacks [return]
77. I've lost attribution but in discussion a few years ago, IRA cells were discovered in the 90s by analysing mobile phone billing records to look for "cliques" of up to five phone numbers which basically only-ever called each other; more details at https://alecmuffett.com/article/14842 [return]
78. *Security of Symmetric Encryption against Mass Surveillance*: https://eprint.iacr.org/2014/438.pdf [return]
79. *Facebook Password Hashing & Authentication*: https://www.youtube.com/watch?v=7dPRFoKteIU [return]
80. *SIM swap scam*: https://en.wikipedia.org/wiki/SIM_swap_scam [return]
81. *How hackers can use message mirroring apps to see all your SMS texts and bypass 2FA security*: https://theconversation.com/how-hackers-can-use-message-mirroring-apps-to-see-all-your-sms-texts-and-bypa [return]
82. or at least non-public [return]
83. *COVID-19: new offences of organising illegal gatherings*: https://uk.practicallaw.thomsonreuters.com/w-027-1998 [return]
84. *Petraeus reportedly used draft e-mails to converse with mistress*: https://www.cnet.com/news/privacy/petraeus-reportedly-used-draft-e-mails-to-converse-with-mistress/ [return]
85. *Here's the e-mail trick Petraeus and Broadwell used to communicate*: https://www.washingtonpost.com/news/worldviews/wp/2012/11/12/heres-the-e-mail-trick-petraeus-and-broadv [return]
86. *The Terrorist's Tricks and Counter-Measures*: https://www.pbs.org/wgbh/pages/frontline/shows/front/special/techsidebar.html [return]
87. *How do terrorists communicate?*: https://www.bbc.co.uk/news/world-24784756 [return]
88. *Online Safety Bill will … prevent underage access … by using age verification technologies*: https://www.gov.uk/government/news/world-leading-measures-to-protect-children-from-accessing-pornograph [return]
89. *UK.gov threatens to make adults give credit card details for access to Facebook or TikTok*: https://www.theregister.com/2022/02/08/age_verification_for_social_media_ukgov_plans/ [return]
90. *What is the eIDAS Regulation?*: https://ico.org.uk/for-organisations/guide-to-eidas/what-is-the-eidas-regulation/ [return]
91. *EU's Digital Identity Framework Endangers Browser Security*: https://www.eff.org/deeplinks/2021/12/eus-digital-identity-framework-endangers-browser-security [return]
92. e.g. social media accounts, phone numbers, PGP keys, Tor Onion Addresses; a principal is the 'hook' or source of truth for an identity within a namespace [return]
93. *Wikipedia: Zero-One-Infinity*: https://en.wikipedia.org/wiki/Zero_one_infinity_rule [return]
94. *Wikipedia: Optic Nerve (GCHQ)*: https://en.wikipedia.org/wiki/Optic_Nerve_%28GCHQ%29 [return]
95. *Wikipedia: LOVEINT*: https://en.wikipedia.org/wiki/LOVEINT [return]
96. *Europe says yes to messaging interoperability as it agrees on major new regime for Big Tech*: https://techcrunch.com/2022/03/24/dma-political-agreement/ [return]

97. Aside: I find it revelatory to consider that perhaps the *digital market* which the DMA wants to open is *access to existing users of big platforms*, as if the people who use Google, Facebook, Amazon, etc, are cattle and are currently insufficiently exploited… by EU corporations [return]
98. *Breaking Up "Ma Zuck": how a generational divide … imperils the deployment of end-to-end encryption as a platform solution for everyone*: https://alecmuffett.com/article/16086 [return]
99. *Wikipedia: OpenOffice.org*: https://en.wikipedia.org/wiki/OpenOffice.org [return]
100. *Wikipedia: Apache OpenOffice*: https://en.wikipedia.org/wiki/Apache_OpenOffice [return]
101. *Wikipedia: OpenOffice.org XML*: https://en.wikipedia.org/wiki/OpenOffice.org_XML [return]
102. *Wikipedia: Embrace, extend, and extinguish: Examples by Microsoft*: https://en.wikipedia.org/wiki/Embrace,_extend,_and_extinguish#Examples_by_Microsoft [return]
103. *FSF: OpenDocument, 2010*: https://www.fsf.org/campaigns/opendocument/copy_of_index_html [return]
104. *Wikipedia: Office Open XML: Application Support*: https://en.wikipedia.org/wiki/Office_Open_XML#Application_support [return]
105. *Wikipedia: List of software that supports Office Open XML*: https://en.wikipedia.org/wiki/List_of_software_that_supports_Office_Open_XML [return]
106. at the time of writing and apparently for a long time before [return]
107. *Data Portability Project Vision & Mission*: https://web.archive.org/web/20120822013735/http://wiki.dataportability.org/pages/viewpage.action?pageId=3 [return]
108. *Guidelines on the right to "data portability" wp242rev.01*: https://ec.europa.eu/newsroom/article29/items/611233/en [return]
109. This model of linguistics doubtless displays considerable roughness, ignores nitpicks and edge-cases, and through brevity is necessarily incomplete; but it's good enough for these purposes [return]
110. With integrated payments you could literally even *throw money at someone.* [return]
111. *White Paper: Considerations for Mandating Open Interfaces*: https://www.internetsociety.org/resources/doc/2020/white-paper-considerations-for-mandating-open-interfaces [return]
112. *Document Interoperability*: https://meshedinsights.com/2021/02/16/interoperability/#Document-Interoperability [return]
113. *Messaging Interoperability*: https://meshedinsights.com/2021/02/16/interoperability/#Messaging-Interoperability [return]
114. reminder: *The level of security, including the end-to-end encryption, where applicable, that the gatekeeper provides to its own end users shall be preserved across the interoperable services* [return]
115. plus: regularly updating your software to obtain bug fixes [return]
116. *… neither nor Signal or Telegram are affected in any way…*: https://web.archive.org/web/20220407135207/https://twitter.com/1Br0wn/status/1512065544110759946 [return]
117. *OPINION: What critics get wrong about regulating Big Tech*: https://news.trust.org/item/20220506153752-cer1a/ [return]
118. *Google's constant product shutdowns are damaging its brand*: https://arstechnica.com/gadgets/2019/04/googles-constant-product-shutdowns-are-damaging-its-brand/ [return]
119. *Here's why Google kills so many of its projects*: https://www.androidcentral.com/heres-why-google-kills-so-many-its-projects [return]
120. *i.e. the horse-sized ducks*: https://www.wired.com/2013/02/why-would-i-fight-a-horse-sized-duck/ [return]
121. … or even liberal democracies… [return]
122. *i.e. the hundreds of duck-sized horses?*: https://knowyourmeme.com/memes/horse-sized-duck [return]
123. *Grand jury subpoena for Signal user data, Eastern District of Virginia*: https://signal.org/bigbrother/eastern-virginia-grand-jury/ [return]

124. *Technology preview: Sealed sender for Signal*: https://signal.org/blog/sealed-sender/ [return]