Alice and Bob Don’t Live Here Anymore

Working Paper, Working Title

Eliot Lear
Draft
05/25/25

Abstract

Many in the technical community are alarmed that the UK having recently mandated Apple to provide unfettered access of British user data in iCloud, some worrying about “catastrophic” failures. Government officials may have a very different idea of what a catastrophic failure is. At the same time, a number of lawful intercept mechanisms have been proposed in the literature but not used. There is not just one disconnect, but many, within both government and technical communities. This paper explores the nature of that disconnect, and it proposes a limit approach to address it.

1 Introduction

“Alice and Bob want to have a private, authenticated conversation where the integrity of their communication is unmolested, the existence of which is not even known.” You could imagine this being the first sentence in a communications security course. Alice and Bob are generally subject to all sorts of attacks. The goal of the Internet threat model as defined in RFC 3552, is to protect these two personae or constructs as we introduce new networking features. Core to that model is the assumption that Alice and Bob are worth protecting, not because they are, but because, as the RFC states, “Protecting against an attack when one of the end-systems has been compromised is extraordinarily difficult.” Alice and Bob, therefore, are simplifying assumptions.

The “encryption debate” begins with the notion that Alice and Bob might not be such nice people. they could be involved in murder for hire, exchange of child sexual abuse material (CSAM), drug trafficking or terrorism. In a social context, our endpoints can indeed be compromised. Lawful intercept (LI) is based on this notion. For decades, a debate has raged over how to improve the Internet threat posture in a way that strengthens end-to-end security, but also provides means to identify malicious content and bad actors. Numerous policy papers have provided both situational assessments and policy recommendations [1,2,3,4]. The discourse between policy makers, law enforcement, and the technical community seemingly has not gone well. Why might this be?

The ability and responsibility of telecommunications providers to report information to law enforcement dates back nearly to the invention of the telephone, when operators could easily listen into calls. In more modern times, this ability has been instantiated at the network layer through functionality enabled in amongst other ways, through SNMP MIBs [RFC3924]. In yet more modern times, as a result of social backlash, requests for access to individual information has become the subject of transparency reports, such as The Google Transparency Report.[5]

This level of *lawful* access has proven not to be enough for some.

- In 2013, we witnessed the U.S. National Security Agency attack Google and Yahoo, as well as the open standards process.[6]
- In September of 2024, the Wall Street Journal reported a broad attack against U.S. service providers, *Salt Typhoon,* through the lawful intercept interfaces by China, who gained access to "meta-data" such as call records, and IP addresses, as well as SMS texts exchanged through the providers.

- In February of 2025, the United Kingdom's Home Office issued a secret order that purportedly requires Apple Computer to disclose on demand all information that anyone in the world has uploaded to their iCloud service.[7]

In two of these cases, we see demonstrations of *unlawful* intercept, vividly demonstrating points made by the authors of [2] through the violation of privacy of millions of innocent Bobs and Alices.[8] In the UK case, one imagines that it is only a matter of time before history repeats itself.

After the Snowden Disclosures, tech companies began to respond to pervasive surveillance through the broader use of encryption, most notably through HTTP2; the IETF labeled pervasive surveillance a threat.[9]

At the same time, we continue to hear the persistent mantra of "You can't give the keys to the good guys and not give them to the bad guys"; sometimes being called a law of physics. But it's not. The issues raised in [2] are real, but are *not* themselves proven laws of physics, and *may* be surmountable. However, none of the approaches that make improvements have been picked up by governments, and the advice given by multiple security experts has not been taken.

What has gone wrong? There are at least four possibilities:

- Policy makers are willing to accept risks to the Internet infrastructure that security experts are not;
- Policy makers are unaware of the concerns of security experts;
- Policy makers do not trust or believe the security experts and industry leaders;
- Current research does not meet requirements of societies.

This rest of this paper explores these factors, and is organised as follows:

- Section 2 discusses different perceptions of risk, and the actual problems people are trying to solve.
- Section 3 tests the claim that "giving the keys to the good guys gives the keys to the bad guys".
- Section 4 discusses a trust gap between security experts, industry leaders, policy makers, and law enforcement.
- Section 5 discusses whether law enforcement needs are well understood.
- Section 6 discusses possible next steps.

2 What's an acceptable risk, and to whom?

Academically, the basic formula for expected loss is well know as:

$$EL = \sum_{i=1}^{n} P_i \cdot L_i$$

Where *EL* is the expected loss, P_i is the probability of loss, and L_i is the Magnitude of loss, for each event *i* for a number of events, *n*. A wide range of academic work has been devoted to calculating cyber losses. However, most of that work has focused on enterprise risk. The cyber insurance market has looked at broad based enterprise loss, and in 2019 one paper predicted an annualized aggregate loss in a 1-100 year event in the United States at $14.6 billion, with the costliest scenario being estimated at $23.6 billion. To put this into context, in 2024, the *Crowdstrike* event alone is said to have cost Fortune 500 Companies alone $5.4 billion in **direct** losses.[10,11] This loss was proximate to the event, and therefore causality could be established, a conclusion not so easily drawn in other situations. Would you be able to determine that I stole your marketing plans, based on the results of my own campaign to negate those plans? Causality is always a tricky problem. *Any* loss will be difficult to calculate, much less aggregates of loss.

In addition, the details will matter. Does the loss require physical access of a device? Does it require that the legitimate user be tricked into doing something to cause a loss? Surreptitious "Zero Click" exploits have taken place on mobile devices.[12,13] Such attacks have generally required at least a message to be delivered to the user's device that would be interpreted by the operating system. The author is unaware of a broad attack that has succeeded, but the risk exists.

One form of loss previously considered was loss of confidence in the infrastructure: would consumers stop using the Internet or eCommerce in the face of director or indirect losses? While research indicates that consumers were likely to reduce their spending after suffering a cybersecurity attack [14], when a break-in is systemic, as was the case with *Salt Typhoon*, the they has few market alternatives to take action against their provider. Therefore this form of loss may be *nil*, which will also be the case for any other concentrated or regulated market.

Security experts argue that over time that the likelihood of a software failure approaches 1, because software is known to fail. At some point in any extraordinary access system, there will be failures.

However, the scope of failure may or may not lead to an incident. Thus the likelihood of a software failure will be a component aspect of P_i, but the two values do not necessarily equate. The Common Vulnerability Scoring System (CVSS) value demonstrates this point. There also exists a budding industry to protect against common software failures, even at runtime, ranging from stack protection to runtime code path verification.

Mechanisms will matter in how we evaluate risk. For instance, if an end system is designed as the point at which access is granted and where proofs are made for that access, the risk might be viewed as incremental, in that end systems suffer many many such vulnerabilities, and an LI vulnerability would just be one more to address. But when a single key can is stored *off box*, such as what happened with *Salt Typhoon*, those management systems can be, and have been, targeted. Mitigations to such attacks should be explored (an example is given below). Attempts have been made to quantify the *Salt Typhoon* loss, ranging as high as $15 billion in a single year.[15] One question is whether service providers and governments understood the risk they were taking. If they were, given that the mechanisms have been in place for over 20 years, the cost can be amortized. Another question is whether we will be able to associate a particular loss with that particular event.

In summary, while some components in the system are likely to fail over time, the scope of the failure is unpredictable, and a loss may be either sustainable or unrecognizable over long periods of time. In short, we cannot easily quantify expected loss or align risks within a society.

This leads us to another aspect of this question: expected loss of a mechanism's presence must be balanced against the expected loss of that mechanism's absence (marginal gain/loss). This is particularly difficult for non-monetary loss, such as online child exploitation, a risk that frequently arises in these debates. Moore and Clayton showed us early on that remediation of ills requires an economic motivation, with child online exploitation lagging far behind other mischief.[16] Nevertheless, Apple attempted to address imagery containing child sexual abuse material (CSAM) through the use of what they called a NeuralHash algorithm, which attempted to spot such images even if they had subtle modifications. That system was withdrawn over privacy concerns due to possible hash collisions leading to false reports and the fact that the process ran on the end device.[17] From a law enforcement perspective, that may well have been viewed as a commercial decision.

Coupled with intangibles and other motivations, a policy maker's understanding of loss will almost certainly not match a security expert's, *on either side of this equation.* With privacy being an intangible, its value will fluctuate with the attitudes of societies. The COVID pandemic brought with it a host of compromises that many consumers were willing to make involving co-location, for instance.[18]

3 Does giving the keys to the good guys also give them to the bad guys?

It is a common statement from security professionals that you can't create a backdoor just for the good guys, for sooner or later the bad guys will find it as well. But does this hold true for lawful intercept mechanisms? At least some research exists that looks at ways to safeguard lawful intercept mechanisms. The following is a hopefully incomplete summary of works that address exceptional access in one way or another, patents excluded:

- In 2014, Joshua Kroll, Ed Felton, and Dan Boneh examined a number of approaches that extend the use of cryptography to apply to lawful intercept.[19]
- In 2015, Adam Bates et. al. described an audit mechanism for lawful intercept requests and answers. Identifying unauthorized access is critical to shutting it down and fixing the mechanism that led to it.[20]
- In 2017, Shafi Goldwasser and Sunoo Park presented an auditing approach through the use of block chains to provide for publicly auditable record keeping while maintaining the secrecy of records. This provides proof of delivery of records kept when a lawful order is presented, and a means to audit how governments are using their authority.[21]
- In 2018, Charles Wright and Mayank Varia presented per-object decryption "crumpled" session keys, with the intent of only providing targeted, not broad scale, access. [22]
- In 2018, Stefan Savage proposed a proof of possession-based model with a time lock to provide extraordinary access to law enforcement.[23]
- In 2020, Sacha Servan-Schreiber and Archer Wheeler developed a delegated trust approach that provides for sharing responsibility for disclosure amongst multiple agencies.[24].
- In 2021, Gulshan Kumar, Rahul Saha, et al presented a blockchain-based framework for evidence gathering from IoT devices in a cross-border environment.[25]

- In 2023, Meng Li, Yifei Chen, et al presented an anonymous blockchain-based approach for vehicular digital forensics, with a temporary reveal for those holding a warrant.[26]
- In 2024, Christian Lindenmeier, Jan Gruber, and Felix Freiling proposed what they classed as a partial solution to lawful intercept through the use of secure access to trusted elements. [27]

On the whole, the authors of these papers were not *advocating* wiretapping or extraordinary access, but were seeking ways to accomplish the task safely with limited harm to others. This author takes no position on the quality of the methods mentioned, but notes their existence. Some of these mechanisms have received additional critique. It is likely none of them comprehensively addresses the needs of law enforcement for two reasons:

1. The needs of law enforcement are neither monolithic nor otherwise crisply identified.
2. The different sets of problems (data in flight, data at rest on a device, and data at rest on a server) may not lend themselves to common solutions.

It is certainly not reasonable to expect law makers or even their staff to understand the above works. What's less clear is whether the security community has some understanding of where the state of the art actually is. Absent that, they may be making outdated claims, or settling into an unwarranted orthodoxy, where science becomes dogma.

This has happened in in another context, and it was an interdisciplinary failure between scientists. During the early days of the COVID pandemic, WHO doctors dismissed the concerns raised by a well published and well known expert on aerosols based on their own mistaken understanding of how far the virus could travel in the air, when it turned out they themselves had no scientific basis for their own views.[28] Thus dogma led to the sort of public policy mistakes that fueled public mistrust of scientists. A 2013 study on mutual trust or distrust between healthcare researchers and policy makers found that time is a key factor for everyone.[29] It takes effort to perform a translation, and *one must trust the translator.* That study found that found that trust was lacking. It may be lacking here as well.

4 What are the limits of trust between policy makers and Big Tech?

It is, in some sense, natural for law enforcement personnel to be sparing of trust, but this too has risks if officers are not well trained on technology. In 2008, Michael Fiola was charged with possessing child pornography, when it was later shown that a virus was responsible for turning his Massachusetts Department of Industrial Accidents (DIA) computer into a repository without his knowledge. Mr. Fiola was fired, and was unable to recoup damages, in spite of past similar cases, with some in law enforcement resorting to referring to this case as a "SODDI defense" (some other guy did it).[30] This case was egregious in that the investigation showed that the computer was making 40 requests per second for illicit material, far beyond any human's capability.

It is important not to overgeneralize. Just because law enforcement got it wrong in the case in Massachusetts doesn't mean they normally make these sorts of mistakes. This is especially so for the Fiola case which took place some decades ago. The only constant we argue here is change. Some examples of that change include the following:

- Intermixing local and remote (cloud) processing;

- Economic viability and use of trusted elements on central processors;
- Improvements in programming methodologies and tooling to reduce security risks;
- Accepting of software updates on a more regular basis in some – but not all – sectors of society;
- Diffusion of Internet-capable devices throughout all sectors of society; and
- Basic scientific advances in the areas of cryptography, physics, and mathematics.

Each of these factors has had some impact on privacy, criminal behavior, and law enforcement. Because of this, ongoing capacity building in the form of technology capabilities and training becomes all the more critical. What was considered dispositive proof yesterday may merely be suggestive today. For instance, Flores et. al. found that false positives in forensic DNA analysis increase when there is less genetic diversity among the samples.[31] Similarly, what was technologically sound advice yesterday may need to evolve as well.

Since expected loss is difficult to account, policy makers might choose to simply believe that it doesn't exist, and therefore question *any* expert about the risk of loss. Out of sight, out of mind. Researchers working in aggregates also pose a different credibility risk: if one claims that *all* law enforcement mechanisms are equally catastrophic, either that statement must be backed by some form of proof, or it must hold true over time.

As mentioned above, many in the research field believe that providing extraordinary access mechanisms of any form incurs unacceptable societal risk. Implicit in that claim is that research has been performed to show that this is so. A simple counter-example can expose such a claim to broad skepticism of those making it. The mechanisms cited in this paper demonstrate at least some work in the field to address both security expert concerns while providing governments some form of privileged access. That in turn validates a comment made by President Obama in 2016:

> *Now, what folks who are on the encryption side will argue is any key whatsoever, even if it starts off as just being directed at one device could end up being used on every device. That's just the nature of these systems. That is a technical question. I'm not a software engineer. It is, I think, technically true, but I think it can be overstated.*[32]

Researchers themselves lament the lack of work that has gone on in the field. To quote but one (and not the only one):

> *To date, the research community has made little progress on improving this state of affairs. While there are many in the community who have strong feelings on the topic, much of this energy has focused on the policy aspects of the debate and there has been comparatively little constructive engagement with the underlying technical questions and options. Absent broad explorations of the technical design space or concrete engineering proposals to focus attention, the issue has become highly polarized—evidenced on both sides by loaded terminology (e.g., "going dark" vs "backdoors"), appeals to authority, and refutations of "straw man" arguments.*[*ibid*]

Another factor has also crept in that has eroded trust between the public and private sector. As early as 2010, a fight had been brewing between cloud providers and Internet service providers, in which the former had been attempting to either view or modify customer data flows. The best example of this was Verizon who, who the FCC eventually fined for introducing "supercookies".[33] While interception and rewriting of requests was invasive and could lead to unexpected browser behaviors, at least one large provider, Google, recognized privacy and profit would work hand in glove if they could "protect" consumers while cornering the advertising and demographics market. To assure their position, Google pushed heavily for encryption of all communications, a drive that

only accelerated after the Snowden revelations. Later they took an additional step to limit so-called tracking cookies in the name of privacy, spurring on multiple investigations[34,35]. Apple's CEO Tim Cook was next. With the FBI's demand that Apple open the iPhone 5s of the Orange County Bomber, Cook refused,[36] While Apple's marketing of privacy might appeal to the consumer, it understandably does not appeal to the law enforcement community, and it may well have limited trust between the parties. In the case of Orange County it was reported that the FBI made use of a third party service to gain access to the phone.[37]
Law enforcement has demonstrated similar successes without the need for the sort of extraordinary access that they have demanded:

- In June of 2021, US, Australian, and European authorities announced the arrest of 500 people who were operating across 100 countries in Operation Trojan Shield, which made use of specially hacked cell phones that revealed communications directly to authorities.[38]
- In March of 2023, Australian and US authorities announced the arrest of 12 people and the interception of $677 million worth of cocaine in Operation Beech.[39]
- Indeed the impetus for [21] was solved by the FBI eventually making use of a private contractor to break into an iPhone.

There are many more such examples that lead researchers to wonder, why does law enforcement need additional capabilities? This is indeed a question for law enforcement to answer. However, it would be a mistake to extrapolate the above to conclude that law enforcement requires no additional authority or capability, as most security researchers are not law enforcement experts who would best understand their needs, in the same way that most policy makers and members of the law enforcement community are not the computer security researchers who best understand capabilities and limitations of the technology. Even putting that distinction aside, extrapolation that *some* investigations can be solved without extraordinary does not imply that *all* investigations can be solved in the same manner. For example, in each of the three above examples, luckily time was not a critical factor.

5 Does the current state of the art meet society's needs?

Each of the papers listed above is intended to meet some use by law enforcement, but just as the state of the art is evolving, so too is the threat environment for societies, who face an ever-evolving set of challenges, from day-to-day criminal behavior by individuals to gang behavior, to government-sponsored, well-funded, and well-organized advanced persistent threats. Even as this paper is being written, there are demonstrations of how the threat is evolving.[40] The research listed above also focuses primarily on well targeted searches. Detection of terrorist activities that at the same time respects privacy remains illusive.

One glaring question that is raised in [22] is that of targeting. Any mechanism specified for use within Sweden might also be used by Russia. Mechanisms used to detect CSAM might also be used to violate human rights. Some of the research above discusses transparency and auditing mechanisms. Can they be employed to identify inappropriate use?

Another glaring question, perhaps a straw man, to address is this: how "perfect" of a solution does law enforcement need? A common argument made by researchers is that because encryption is relatively easy to implement and deploy, even if law enforcement is given access at one layer, they may only decrypt information at that layer to find that it has been encrypted at the layer above. This is not, as they say, rocket science. Here I posit that we run into two problems:

1. No investigator likes to openly discuss means and methods, lest Bad Guys[1] take advantage of this knowledge to evade detection. The success of keeping those means and methods hush hush was demonstrated in the previous section, but what happens when the cat is out of the bag? The computer security expert's answer to law enforcement is to do detective work (the equivalent of "nerd harder").
2. At the same time, because the means and methods in these situations risk weakening of overall security, the most commonly accepted way to avoid those risks is open discussion of the approach to be taken.

CSAM detection in particular raises substantial risks, because it typically involves having access to both targeted and untargeted sets of data. When one seeks a warrant, in most societies that warrant is targeted at a specific data set. The mechanisms discussed above **mostly** address targeted sets of data.

This leaves open a question for policy makers and law enforcement? What access is good enough?

There have been attempts at these sorts of discussions, off and on. As mentioned above, the Carnegie Endowment hosted an expert group to propose a framework for addressing lawful intercept requirements. The Internet Society and Chatham House held a roundtable discussion on this topic in 2017.[41] Similar roundtables have occurred over time. However, none seem to have had a sustained engagement. One can only conjecture as to why that is, given that these activities often occur under the Chatham House Rule that participant names are not disclosed.

6 Conclusion and Next Steps

The basis of this paper is the endpoints Bob and Sally may not be doing good things. From this garbled view, we can conclude a few things: first, it is difficult to establish a loss model that policy makers and law enforcement would willingly accept, as these groups view loss not strictly in economic terms. Second, if the potential economic risk is understood, at the very least it can be amortized (we call this an insurance market). Third, there does exist at least some research that might lead to safer disclosure models, but it is fragmented and limited. Simply saying "giving the keys to the good guys gives the keys to the bad guys" is dogmatic at best. Fourth, perfect may be the enemy of good and friend of bad: governments have shown that they will not wait for perfect. Finally, researchers and policy makers do not have a common understanding of evolving threat models and different policy goals, and only limited communication occurs between the parties. This is particularly true across jurisdictions, a notable challenge when communications cross them.

In the Internet, we like to try running code and see what happens. This is what the UK is doing right now, risks and all. But it may be better to try **different** running code in different contexts to compare results. This leads to a few follow-on questions:

- Can some of the above research be organized into a coherent response to specific policy goals?
- Can a governance model be established such that extraordinary access can be managed across likeminded jurisdictions? The Council of Europe's Budapest Convention is an example of this, but it has not been shown to address the problems discussed in this paper, and it does not substantially engage the technical community. Could it or another vehicle be developed?

1 The use of the term "Bad Guys" is meant in a classical historic context.

- Could the above two points be tested across a small group of jurisdictions to find happy mediums instead of governments applying broad powers that might entail heavy risks?
- Finally is there a neutral venue to discuss these possibilities where in which interested parties can engage?
- What are the criminology aspects that need further studying with any model?
- On the Internet the popular “devops” model allows for continuous improvement. Try a little, change a little, improve a little each time. Policy making is, by its nature, **not** agile. How might these two worlds meet to address law enforcement needs while improving mechanism over time?
- And how can risk be characterized as these mechanisms are developed?

This paper has looked primarily at the problem space. The above bullets are meant as next steps, without drawing strong conclusions. That is up to a collaborative effort amongst researchers, law enforcement, policy makers, and other interested parties. The alternative is poorly understood risks to society.

1 L. Geierhaas, F. Otto, M. Häring, and M. Smith, “Attitudes towards Client-Side Scanning for CSAM, Terrorism, Drug Trafficking, Drug Use and Tax Evasion in Germany,” 2023 IEEE Symposium on Security and Privacy (SP), pp. 217–233, May 2023, doi: https://doi.org/10.1109/sp46215.2023.10179417.

2 H. Abelson *et al.*, “Keys under doormats,” *Communications of the ACM*, vol. 58, no. 10, pp. 24–26, Sep. 2015, doi: https://doi.org/10.1145/2814825.

3 J. Baker, K. Charlet,, *et. al.*,“Moving the Encryption Policy Conversation Forward,” *Carnegie Endowment for International Peace*, 2019. https://carnegieendowment.org/research/2019/09/moving-the-encryption-policy-conversation-forward (accessed Feb. 22, 2025).

4 I. Levy and C. Robinson, “Principles for a More Informed Exceptional Access Debate,” *Lawfare*, Nov. 29, 2018. https://www.lawfaremedia.org/article/principles-more-informed-exceptional-access-debate (accessed Feb. 22, 2025).

5 “Google Transparency Report,” *transparencyreport.google.com*. https://transparencyreport.google.com (accessed May 25, 2025).

6 G. Greenwald, “NSA Collecting Phone Records of Millions of Verizon Customers Daily,” *The Guardian*, Jun. 06, 2013. https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (accessed Feb. 22, 2025).

7 J. Menn, “U.K. orders Apple to let it spy on users’ encrypted accounts,” *Washington Post*, Feb. 07, 2025. https://www.washingtonpost.com/technology/2025/02/07/apple-encryption-backdoor-uk/ (accessed Feb. 22, 2025).

8 S. Krouse, R. McMillan, and D. Volz, “Chinese-Linked Hackers Breach U.S. Internet Providers in New ‘Salt Typhoon’ Cyberattack,” *The Wall Street Journal*, Sep. 25, 2024. https://www.wsj.com/politics/national-security/china-cyberattack-internet-providers-260bd835.

9 S. Farrell and H. Tschofenig, “Pervasive Monitoring Is an Attack,” *RFC 7258*, May 2014, doi: https://doi.org/10.17487/RFC7258.

10 K. O’Flaherty, “CrowdStrike Reveals What Happened, Why—And What’s Changed,” *Forbes*, Aug. 07, 2024. Available: https://www.forbes.com/sites/kateoflahertyuk/2024/08/07/crowdstrike-reveals-what-happened-why-and-whats-changed/

11 S. Snider, “CrowdStrike Outage Drained $5.4 Billion from Fortune 500: Report,” *Informationweek.com*, Jul. 30, 2024. https://www.informationweek.com/cyber-resilience/crowdstrike-outage-drained-5-4-billion-from-fortune-500-report

12 Apple, Inc., “Vulnerability Report CVE-2023-41064,” *Mitre*, Sep. 07, 2023. https://www.cve.org/CVERecord?id=CVE-2023-41064The Chicago man charged ith killing two Israeli Embassy staffers has been a vocal advocate for Palestinian issues and a staunch critic of corporations.

13 Apple, Inc., “Vulnerability CVE-2023-41061,” *Mitre*, Sep. 07, 2023. https://www.cve.org/CVERecord?id=CVE-2023-41061

14 R. Bohme and T. Moore, “How do consumers react to cybercrime?,” *2012 eCrime Researchers Summit*, pp. 1–12, Oct. 2012, doi: https://doi.org/10.1109/ecrime.2012.6489519.

15 L. Sydow, “Salt Typhoon Telecom Hack Rattles Critical Infrastructure,” *Interos*, Dec. 11, 2024. https://www.interos.ai/salt-typhoon-telecom-hack-rattles-critical-infrastructure/

16 T. Moore and R. Clayton, “The Impact of Incentives on Notice and Take-down,” *Springer eBooks*, pp. 199–223, Dec. 2008, doi: https://doi.org/10.1007/978-0-387-09762-6_10.

17 S. K. Lim, “Apple’s NeuralHash — How it works and how it might be compromised,” *Medium*, Aug. 20, 2021. https://medium.com/towards-data-science/apples-neuralhash-how-it-works-and-ways-to-break-it-577d1edc9838 (accessed Mar. 07, 2025).

18 S. Lewandowsky *et al.*, “Public acceptance of privacy-encroaching policies to address the COVID-19 pandemic in the United Kingdom,” *PLoS ONE*, vol. 16, no. 1, Jan. 2021, doi: https://doi.org/10.1371/journal.pone.0245740.

19 J. Kroll, E. Felten, and D. Boneh, “Secure protocols for accountable warrant execution,” Apr. 2014. Accessed: Feb. 23, 2025. [Online]. Available: https://www.cs.princeton.edu/~felten/warrant-paper.pdf

20 A. Bates, K. R. B. Butler, M. Sherr, C. Shields, P. Traynor, and D. Wallach, “Accountable wiretapping – or – I know they can hear you now,” *Journal of Computer Security*, vol. 23, no. 2, pp. 167–195, Jun. 2015, doi: https://doi.org/10.3233/jcs-140515.

21 S. Goldwasser and S. Park, “Public Accountability vs. Secret Laws: Can They Coexist?,” *Proceedings of the 2017 Workshop on Privacy in the Electronic Society*, pp. 99–110, Oct. 2017, doi: https://doi.org/10.1145/3139550.3139565.

22 C. Wright and M. Varia, “Crypto Crumple Zones: Enabling Limited Access without Mass Surveillance,” *IEEE Xplore*, Apr. 01, 2018. https://ieeexplore.ieee.org/abstract/document/8406606 (accessed Nov. 18, 2021).

23 S. Savage, “Lawful Device Access without Mass Surveillance Risk,” *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1761–1774, Jan. 2018, doi: https://doi.org/10.1145/3243734.3243758.

24 S. Servan-Schreiber and A. Wheeler, “Judge, Jury & Encryptioner: Exceptional Device Access with a Social Cost,” *arXiv (Cornell University)*, Jan. 2019, doi: https://doi.org/10.48550/arxiv.1912.05620.

25 G. Kumar, R. Saha, C. Lal, and M. Conti, “Internet-of-Forensic (IoF): A blockchain based digital forensics framework for IoT applications,” *Future Generation Computer Systems*, vol. 120, pp. 13–25, Jul. 2021, doi: https://doi.org/10.1016/j.future.2021.02.016.

26 M. Li, Y. Chen, C. Lal, M. Conti, M. Alazab, and D. Hu, “Eunomia: Anonymous and Secure Vehicular Digital Forensics Based on Blockchain,” *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 1, pp. 225–241, Jan. 2023, doi: https://doi.org/10.1109/tdsc.2021.3130583.

27 C. Lindenmeier, J. Gruber, and F. Freiling, “InvesTEE: A TEE-supported Framework for Lawful Remote Forensic Investigations,” *Digital Threats: Research and Practice*, pp. 1–20, Jul. 2024, doi: https://doi.org/10.1145/3680294.

28 M. Molteni, “The 60-Year-Old Scientific Screwup That Helped Covid Kill,” *Wired*, May 14, 2021. Accessed: Feb. 23, 2025. [Online]. Available: https://www.wired.com/story/the-teeny-tiny-scientific-screwup-that-helped-covid-kill/

29 S. E. Gollust, J. W. Seymour, M. J. Pany, A. Goss, Z. F. Meisel, and D. Grande, “Mutual Distrust: Perspectives From Researchers and Policy Makers on the Research to Policy Gap in 2013 and Recommendations for the Future,” *INQUIRY: The Journal of Health Care Organization, Provision, and Financing*, vol. 54, Apr. 2017, doi: https://doi.org/10.1177/0046958017705465.

30 D. C. Weiss, “Viruses Can Infect Computers with Child Porn, Leading to Legal Charges,” *ABA Journal*, Nov. 10, 2009. https://www.abajournal.com/news/article/viruses_can_infect_computers_with_child_porn_leading_to_legal_charges (accessed Feb. 23, 2025).

31 M. Flores *et al.*, “Decreased accuracy of forensic DNA mixture analysis for groups with lower genetic diversity,” *iScience*, Sep. 2024, doi: https://doi.org/10.1016/j.isci.2024.111067.

32 B. Obama, “President Obama Speaks at SXSW,” *The Texas Tribune*, Mar. 11, 2016. https://www.texastribune.org/obama-sxsw/ (accessed Feb. 23, 2025).

33 C. Kang, “Verizon Settles With F.C.C. Over Hidden Tracking via ‘Supercookies,’” *The New York Times*, Mar. 07, 2016. Accessed: Mar. 06, 2025. [Online]. Available: https://www.nytimes.com/2016/03/08/technology/verizon-settles-with-fcc-over-hidden-tracking.html.

34 A. Riehl, “Canada’s Competition Bureau targets Google for anti-competitive practices,” *BetaKit*, Nov. 28, 2024. https://betakit.com/canadas-competition-bureau-targets-google-for-anti-competitive-practices/ (accessed Mar. 06, 2025).

35 EIN News, “Google Ad Tech Claim gets green light from UK Competition Appeal Tribunal,” *EIN News*, Mar. 05, 2025. https://tech.einnews.com/pr_news/791231499/google-ad-tech-claim-gets-green-light-from-uk-competition-appeal-tribunal (accessed Mar. 06, 2025).

36 L. Kahney, “The FBI wanted a backdoor to the iPhone. Tim Cook said no,” *Wired*, Apr. 16, 2019. https://www.wired.com/story/the-time-tim-cook-stood-his-ground-against-fbi/

37 L. Segall, J. Pagliery, and J. Wattles, “FBI says it has cracked terrorist’s iPhone without Apple’s help,” *CNNMoney*, Mar. 28, 2016. https://money.cnn.com/2016/03/28/news/companies/fbi-apple-iphone-case-cracked/index.html (accessed Mar. 09, 2025).

38 United States Attorney's Office, Southern District of California, “FBI’s Encrypted Phone Platform Infiltrated Hundreds of Criminal Syndicates; Result is Massive Worldwide Takedown,” *www.justice.gov*, Jun. 08, 2021. https://www.justice.gov/usao-sdca/pr/fbi-s-encrypted-phone-platform-infiltrated-hundreds-criminal-syndicates-result-massive (accessed Feb. 23, 2025).

39 Reuters, “International drug bust nets $677 million of cocaine bound for Australia,” *CNN*, Mar. 04, 2023. https://edition.cnn.com/2023/03/04/australia/cocaine-drug-bust-australia-us-intl/index.html (accessed Feb. 23, 2025).

40 D. Black and Google Threat Intelligence Center, “Signals of Trouble: Multiple Russia-Aligned Threat Actors Actively Targeting Signal Messenger,” *Google Cloud Blog*, Feb. 19, 2025. https://cloud.google.com/blog/topics/threat-intelligence/russia-targeting-signal-messenger/ (accessed Feb. 23, 2025).

41 The Internet Society, “Internet Society-Chatham House Roundtable on Encryption and Lawful Access,” *Internet Society*, Oct. 17, 2017. https://www.internetsociety.org/resources/doc/2018/internet-society-chatham-house-roundtable-on-encryption-and-lawful-access/ (accessed Feb. 23, 2025).