A Milestone in Encryption Control – What Sank the US Key-Escrow Policy?

Craig Jarvis[a]* and Keith M. Martin[b]

[a]*Independent Researcher, craiginfosec@gmail.com; Information Security Group, Royal Holloway, University of London, United Kingdom, keith.martin@rhul.ac.uk;* [b]

Author Bios

Craig Jarvis is an international security researcher who holds a PhD in cyber security and history from Royal Holloway, University of London. He is a guest lecturer at Royal Holloway and Oxford, author of *Crypto Wars* and a contributing author to *Next-Generation Enterprise Security and Governance*.

Prof. Keith Martin is a professor of information security at Royal Holloway, University of London. His research interests include cryptography and geopolitical aspects of cyber security. He is author of the textbook *Everyday Cryptography* and *Cryptography: The Key to Digital Security, How it Works and Why it Matters*.

A Milestone in Encryption Control – What Sank the US Key-Escrow Policy?

In the 1990s, the US government recognised its citizens required cryptography for protection of digital data but also that encryption may impede law enforcement and intelligence collection. To reconcile these, President Clinton introduced the key-escrow policy, whereby the state would provide citizens with powerful encryption software whilst retaining decryption capabilities. The policy ultimately failed - the determinant reason for its discontinuation is unknown. This article posits and evidences that industry's argument that key-escrow would curtail the global growth of the US technology sector was the determinant factor in the policy's discontinuation.

Keywords: Key-escrow; clipper chip; crypto-wars; digital surveillance; encryption; exceptional access.

Introduction

Intelligence success depends upon data access, but encryption impedes this access.[i] While encryption historically required expertise to apply, today software habitually applies encryption to internet traffic without users being aware. This reality was not preordained. For half-a-century governments, corporations, and citizens have battled over encryption's democratisation, a conflict branded the 'crypto-wars'.[ii]

During the mid-twentieth century governments held a cryptographic monopoly. Yet, by Clinton's inauguration, the fear that encrypted digital communications could facilitate an ungoverned space beyond the state's reach was established.[iii] Whilst digital represented only one intelligence source, the Clinton administration, including 'Information Super-Highway' champion vice-president Al Gore, likely recognised the importance of its preservation.

In the early 1990s, commercial cryptography was tightly regulated but these controls were increasingly ineffective in preventing cryptography's propagation. Regulations were concentrated at international transmission points yet acted as de-facto domestic controls since manufacturers, tasked with producing two strengths of cryptography to separately serve domestic and foreign markets, often produced only the weaker of the two, compliant for both domains.[iv]

Privacy activists expected Clinton to ease cryptography regulations, but fears of encryption protecting terrorists was a primary reason this did not happen.[v] Addressing the UN in the aftermath of the 1993 World Trade Center bombing, Clinton stated 'Growing global stockpiles of plutonium and highly enriched uranium are raising the danger of

nuclear terrorism for all nations.'[vi] Privacy activist John Perry Barlow believed that Clinton and Gore were 'convinced that such plots are more likely to ripen to hideous fruition behind a shield of encryption.'[vii] A classified 1992 FBI encryption report stated: 'To permit unregulated use of excellent cryptography would establish an electronic sanctuary for conducting criminal activities, unfettered by legal process.'[viii]

The FBI advocated a national cryptography strategy that 'affords legitimate users of cryptography protection which their adversaries cannot defeat', whilst ensuring 'cryptographic devices and systems are capable of real-time decryption by law enforcement'.[ix] The report did not highlight the consensus within the cryptology community that such a goal was impossible without creating a systemic vulnerability in the digital ecosystem. Controversially, the FBI argued for prohibition of 'cryptography that cannot meet the standard enumerated.'[x] Further, the risk of government abuse was not explored. Cryptographer Phillip Zimmermann articulated this danger to the US Senate in 1996:

> in a democracy, it is possible for bad people to occasionally get elected - sometimes very bad people. Normally, a well-functioning democracy has ways to remove these people from power. But the wrong technology infrastructure could allow such a future government to watch every move anyone makes to oppose it. It could very well be the last government we ever elect.[xi]

The key-escrow proposal was presented to the Clinton national security team in 1993. The initiative advocated producing a government encryption chip to be used within telephones and computers. The first-generation chip, known as 'Clipper', was designed for telephony encryption, later devices would also encrypt computer communications. Federal agencies would store (escrow) decryption keys, releasable to law enforcement

upon production of a court order against the device's owner(s). Stewart Baker, NSA's General Counsel between 1992 and 1994, recalls Gore commenting, 'everything else requires very difficult compromises and very unsatisfying compromises, and this [key-escrow] elegantly addresses the issue.'[xii]

Literature Review

The existing key-escrow literature is dominated by research contemporaneous with, rather than retrospective to, the policy. The literature is broadly divided into two disciplinary bodies, namely technical analyses, authored mostly by computer scientists,[xiii] and legal analyses, written predominantly by lawyers.[xiv] Across these works, four major policy challenges that represent potential contributors to the policy's failure are identified:

1. the advancement of public cryptography knowledge[xv];
2. legal challenges against the constitutionality of existing encryption regulations[xvi];
3. domestic legislative misalignment[xvii]; and
4. industry concerns that key-escrow would curtail its global growth[xviii].

The existing literature offers limited assessment as to the extent each of these variables contributed to key-escrow's discontinuation. In 2003, Pednekar-Magal and Shields[xix] posited that the intra-government conflicts between the executive and Congress may have played an important role in the policy failure,[xx] concluding: 'The White House was aware that if it had not withdrawn the Clipper Chip […] Congress would have done so with the passage of the SAFE [Safety and Freedom Through Encryption] bill.'[xxi] They also suggest that international opposition may have played a role, noting:

> If the administration had found widespread support among these state actors, it may well have been able to persuade Congress to go along with Clipper […].[xxii]

While Pednekar-Magal and Shields offer valuable insights into the demise of key-escrow, they seemingly lacked access to primary source material. The passage of time has enabled primary sources to become more accessible, allowing a re-examination of their assessment.

Key-escrow can be considered a harbinger of surveillance-oriented security technologies (SOSTs), a phenomena prominent from the early twenty-first century. Esposti and Gomez describe SOSTs as 'technologies which collect information about the general population to monitor the activities of potential suspects and to prevent criminal acts from occurring'.[xxiii] Pavone et al. observe that SOSTs were 'developed and deployed in an unprecedented manner' following 9/11 as governments sought to increase homeland security with domestic surveillance. Pavone et al. believe that 'large-scale' use of SOSTs is being 'co-constructed along with a new social order where pre-emptive security approaches consider every citizen as a suspect as long as he or she has not been proven to be innocent'.[xxiv]

Hughes offers similar concerns, arguing SOSTs can induce self-censorship or conformism, a phenomenon known as 'chilling'.[xxv] These concerns echo many of those made during the key-escrow debate.[xxvi] Yet, Bauman et al. argue citizens may be sanguine regarding surveillance. To support this position, they reflect on the public response to the 2013 Snowden disclosures. They comment that whilst the media may have expected 'earthquakes', they instead 'caused slight, hardly felt tremors'.[xxvii]

Bauman et al. do not explore that citizens may respond differently to distinct forms, implementations, and governance of surveillance technologies. A 2015 study by Esposti and Gomez found that participants felt traditional surveillance such as CCTV was considered 'fairly equitable', whereas digital monitoring with its perceived lack of transparency and available public information raised 'serious concerns'.[xxviii] It should also be noted that governments, who Bauman et al. position as benevolent, are not the only end users of surveillance products – companies, such as Alphabet and Meta, whose priorities are driven by profits, also have access to mass-surveillance capabilities.

There are some notable differences between today's SOSTs and key-escrow, principally that key-escrow was not operated for target discovery, but only when probable cause and a judicial warrant were obtained. This mechanism was to be protected by multiple government, and in later iterations, industry, parties escrowing the keys to offer an additional safeguard against system abuse. However, one of the principle challenges for key-escrow was whether citizens could trust the government not to subvert these avowed operational parameters, and whether industry were susceptible to coercion via covert legal instruments (such as would be used post 9-11 to covertly access user data from communications providers),[xxix] or commercial incentives (such as those used to encourage AT&T's key-escrow adoption).[xxx] Despite these differences, key-escrow represents an early example of the attempts to embed surveillance technologies at the heart of the digital ecosystem, a microcosm of a debate that remains prevalent today.

Materials and Methods

This article attempts to provide a more definitive answer as to why the key-escrow policy failed. Through a series of interviews with those involved in the key-escrow policy, we identify new insights into the policy's demise. Several criteria were used to identify potential interviewees. Firstly, primary and secondary sources were reviewed to identify policy participants. Within government this included relevant cabinet secretaries (e.g., Defense and Commerce), as well as intelligence directors, White House employees in digital policy roles, and the Vice President (a prominent key-escrow advocate). Beyond government, influential industry captains were identified, as well as digital NGO leaders and relevant academics. All those approached for interview were asked to recommend further individuals who may be able to help address the research question. In total, 55 interviews were requested between October 2020 and March 2021, with a 30% response rate and just over 20% consenting (see Appendix A).

Semi-structured interviews were assessed as the most suitable method as they provided license to seek expansion of subject responses.[xxxi] Subjects were asked identical questions, with some designed to elicit recollections and others intended to explore the reasons for key-escrow's failure. Question order was maintained with all interviewees unless a strong reason for diverging arose during interview. The interview schedule is included as Appendix B. As these interviews took place during the pandemic, all interviews were conducted using video-conferencing. Interviews were carried out between January and March 2021. All interviewees consented to their responses being published.

Several methodological concerns must be acknowledged. Human sources with government backgrounds may remain beholden to complex classification laws. Whilst sources may be at liberty to talk about some elements, there may be aspects to which they cannot speak. Many sources may have felt compelled to omit information unfavourable to their position to defend what they believe is their professional legacy, or to protect their former employers. Likewise, digital privacy activists may have felt a need to defend their actions and positions. Further, as with any historical research, there is a bias to surviving sources – some perspectives may have been lost to history.

This article also makes use of source material such as legal records, media articles, and archival data, including that in the private holdings of interviewees.

We now discuss each of the policy challenges in turn, before analyzing the new interview content to explore the key influences that likely impacted key-escrow's demise.

Policy Challenges

Challenge I: The Advancement of Public Cryptography Knowledge

During the 1980s, public access to cryptography research and tools greatly expanded as the cryptology community coalesced internationally. In 1981, the first annual academic `Crypto' research conference was held in California. One year later the *International Association for Cryptologic Research* was founded, whose members in 1988 established the *Journal of Cryptology*. By 1990, annual academic cryptography conferences were also being held in the Asian, Australasian, and European regions.[xxxii] The free open-source software (FOSS) movement was also accelerating, with the first stable version of the Linux operating system released in 1994.[xxxiii] The proliferation of cryptographic knowledge and the maturation of FOSS communities had significant implications for the production of open-source cryptography tools. Philip Zimmermann's Pretty Good Privacy (PGP) encryption software, which became a focal point for the FOSS cryptographic community during the early 1990s, is the most prominent example.

Zimmermann's PGP was the first high-profile encryption programme of its kind. Utilising public-key technologies, and free to users, PGP offered citizens new privacy capabilities. PGP's development was accelerated by potential government legislation to curtail the use of encryption, such as the language then-Senator Joe Biden inserted into legislation expressing the view that the government should be able to recover plain text data.[xxxiv] Propagation of PGP posed a threat to key-escrow's viability since encryption tools such as PGP would likely need to become restricted (an approach for which the FBI was lobbying).[xxxv] Whilst there were no laws to prevent US domestic distribution of encryption software, global dissemination without the relevant government licenses was a federal crime. Zimmermann claimed he would only share the code with his fellow US

citizens. Yet, prevention of global dissemination of PGP proved, unsurprisingly, infeasible and PGP spread quickly around the globe.

In 1993, US Customs opened a formal investigation into PGP's export.[xxxvi] Whether this investigation was instigated or encouraged by the NSA, the Clinton administration, local or federal entities is unknown. However, with the timing only two months before the announcement of key-escrow, it is possible Customs were encouraged to open the investigation to help remove perceived obstacles to the policy. The government lacked legislation to prevent domestic distribution of encryption software. Yet, if it could successfully argue that open-source software releases uploaded online equated to effective foreign export, it could potentially retard domestic cryptographic development and dissemination. In 1996, the US Attorney's office in California announced there would be no PGP-related prosecutions.[xxxvii] No reason for terminating the case was given.

Challenge II: Testing the Cryptography Regulations' Constitutionality

For the key-escrow policy to be successful, it was vital that regulations upon which the existing encryption controls relied, principally the International Traffic in Arms Regulations (ITAR), were not adjudged unconstitutional. Three legal challenges to the constitutionality of government encryption regulations took place during the key-escrow period. We summarize these cases only until the point in time at which key escrow was discontinued.

Case I – Bernstein

Daniel Bernstein was first exposed to the encryption export regulations in the early 1990s.[xxxviii] Bernstein recalls 'I heard that the government controlled encryption exports, but that it permitted exports of encryption technology in the form of specialized "one-

way hash functions". This struck me as silly.'[xxxix] Hash functions are cryptographic algorithms enabling data integrity checks, but not encryption. Bernstein thus devised an approach to challenge the export regulations by writing a simple programme, Snuffle, which could convert legally exportable hash functions into encryption mechanisms.[xl]

After several years of Bernstein failing to gain the government's permission to export his code, in February 1995 the Electronic Frontier Foundation (EFF) announced it was sponsoring a Bernstein lawsuit against the State Department.[xli] Bernstein's lawyer, Cindy Cohn, commented that the case, 'simply asks the courts to recognize that the First Amendment [freedom of speech] extends to science on the internet, just as it does to science on paper.'[xlii]

In April 1996, Judge Patel ruled that 'for the purposes of First Amendment analysis, this court finds that source code is speech.'[xliii] A month later Patel affirmed that source code was speech deserving of First Amendment protection, only to be overridden in times of war in order to prevent 'direct, immediate and irreparable damage to our nation', - the government's justification for preventing cryptography 'speech', she stated, did not meet this criteria. Patel highlighted the absence of a time limit on ITAR decisions and the lack of a judicial review provision. Patel judged that the regulation 'acts as an unconstitutional prior restraint in violation of the First Amendment', therefore, it was 'unenforceable', and Bernstein was safe from prosecution.[xliv]

A few months later, President Clinton issued Executive Order 13026, transferring regulation of non-military encryption to the Commerce Department's Commerce Control List (CCL).[xlv] The CCL was an instrument of the Export Administration Regulations (EAR). Violation of the EAR could result in penalties of up to $250,000 and ten years

imprisonment.[xlvi] Cohn took the case back to court, where Judge Patel stated that the new regulations were 'even less friendly to speech than the ITAR.'[xlvii] Patel declared the EAR unconstitutional on the grounds of prior restraint, and gave Bernstein immunity against its enforcement.[xlviii] The Justice Department requested, and was granted, a stay of Bernstein's injunction pending an appeal citing his actions posed 'immediate and irreparable harm on the government's interests.'[xlix] Around this time, the key-escrow policy was discontinued.

Case II - Karn (& Schneier)

Cypherpunk Phil Karn attempted to gain permission to export a digital copy of the source code included within Bruce Schneier's *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, published in 1993.[l] When the 1994 request was made, Schneier's book had sold around fifteen-thousand copies, with over fifteen-hundred selling overseas.[li] The State Department informed Karn that the Applied Cryptography diskette had been designated as an ITAR defence article subject to export controls.[lii]

Karn took the State Department to court, where Judge Charles Richey dismissed the case in March 1996. Richey stated that Karn raises 'meritless constitutional claims because he and others have not been able to persuade the Congress and the Executive Branch that the technology at issues does not endanger the national security.' Richey judged the diskette's export a 'political question'.[liii]

Karn appealed the Richey ruling, but before his case could reach court, Clinton transferred export controls for civilian encryption from the ITAR to the EAR.[liv] A new export request was made of the Commerce Department.[lv] In November 1997, Commerce

informed Karn that the diskette would not be approved for export.[lvi] Around this time, the key-escrow policy was discontinued.

Case III – Junger

In 1993, Law Professor Peter Junger, who believed that lawyers should protect their communications with encryption, wrote his own 'simple' encryption programme, Twiddle, to demonstrate to his students.[lvii] Junger realised that teaching or publishing his encryption programme may be subject to ITAR restrictions since foreign students were often in his class.

Junger engaged with the government to determine whether he could teach cryptography to his students. After receiving only non-committal and ambiguous responses, in August 1996 Junger sought an injunction against the government allowing him to 'Teach, publish and otherwise disclose unclassified cryptographic information to foreign students and other foreign persons without first obtaining a license.'[lviii] Junger's lawyers stated that 'The First Amendment allows Prof. Junger to decide what he wants to teach, how it should be taught and to whom he can teach […] without having to obtain a license.'

Judge Nugent issued a preliminary injunction on behalf of Junger in late 1996, stating that 'There is little, if any, likelihood that disclosures of cryptographic information by Prof. Junger or his students would compromise the national security of the US.'[lix] Nugent ruled the ITAR cryptographic export regulations 'constitute a prepublication registration and licensing scheme that does not provide for judicial review and thus constitute an unconstitutional prior restraint in violation of the First Amendment.' Nugent added that the regulations were 'overbroad and vague […], in violation of the First and Fifth Amendments.'

On November 15, 1996, Clinton transferred the regulation of non-military encryption to the Commerce Department.[lx] In response, Junger's legal team requested the judiciary declare EAR unconstitutional.[lxi] Around this time the key-escrow policy was discontinued.

Challenge III: Domestic Legislative Misalignment

The executive attempted to gain congressional support for their key-escrow policy. From the policy's inception, numerous bills were advanced that either promoted the initiative (e.g. the Anti-Electronic Racketeering Act of 1995) or liberalised cryptography controls (e.g. the Promotion of Commerce On-Line in the Digital Era [PRO-CODE] Act of 1996) - none passed.[lxii] Notably, several of the pro key-escrow draft bills treated the Internet as a foreign (global) dissemination medium. Therefore, the legislation effectively made online dissemination of encryption illegal, and thus also constrained domestic access to cryptography.[lxiii] Advocates of liberalisation increasingly framed their bills as pro-market, rather than simply pro-privacy, such as Senator Burns, who argued that 'Until we get the federal government out of the way and encourage the development of strong cryptography for the global market, electronic commerce and the potential of the internet will not be realized.'[lxiv]

In 1996, a Congress-ordered report entitled: *Cryptography's Role in Securing the Information Society (CRISIS*) was produced by the National Research Council.[lxv] The council assessed that 'Widespread commercial and private use of cryptography in the US and abroad is inevitable in the long run and that its advantages, on balance, outweigh its disadvantages.'[lxvi] The authors concluded 'The overall interests of the government and

the nation would best be served by a policy that fosters a judicious transition toward the broad use of cryptography.'[lxvii] The council assessed that 'current national cryptography policy is not adequate to support the information security requirements of an information society.'[lxviii] Importantly for liberalisation advocates, the recommendations included that 'no law should bar the manufacture, sale, or use of any form of encryption within the US', and that 'national cryptography policy […] should be more aligned with market forces.'[lxix] The council concluded 'Export controls on cryptography should be progressively relaxed but not eliminated.'[lxx]

With the continuing deadlock in Congress, in April 1997, the President's Export Council Subcommittee on Encryption (PECSENC) was formed to further investigate the existing regulation's impact.[lxxi] PECSENC's 1998 report found a 'palpable' commercial impact of export controls: 'For many software applications, business customers simply demand security and encryption; it is a checklist item, and its absence is a deal breaker.'[lxxii] The authors noted many US software companies were embarking upon 'cooperative arrangements' with foreign encryption suppliers able to 'provide complete security solutions by encouraging their foreign partners to marry foreign-made crypto with US commercial applications.' The authors assessed US export policy had 'fostered the development of cryptographic software and hardware skills outside the US. German, Swiss, Canadian, Russian, and Israeli cryptography companies have all benefited from this unintended consequence of US encryption policy.[lxxiii] Whilst gradually tilting towards liberalization, even with the release of these reports Congress remained in gridlock.

Challenge IV: Industry Concerns that Key-Escrow Will Curtail Global Growth

Key-escrow undoubtedly presented a challenge for the technology industry that foresaw the global reach of the Internet as a major source of growth. It was believed by many in industry that if key-escrow were integrated into its product lines, they would be excluded from international markets.[lxxiv]

Several channels existed between industry and the government through which the former lobbied for liberalisation of encryption regulations. Firstly, industry groups produced reports and media to support industry's positions. Secondly, there were private channels between the Clinton administration and the technology firms within which lobbying could occur. Finally, there were individual channels between industry leaders and politicians. We now outline some of the driving engagement forces within the industry community and several key events during the key-escrow period.

Microsoft and RSADSI

Industry's lobbying against key-escrow was dominated by Microsoft,[lxxv] whose approach to lobbying was to accentuate the national economic imperative of cryptographic liberalisation.[lxxvi] Whilst US companies held a 'first-movers' advantage in the industry, should they fail to offer robust security provisions within their products, foreign competitors would soon erode their competitive advantage. Another company relentlessly vocal in its protestations of the encryption policies was cryptography company RSADSI, who entered a strategic partnership with Microsoft in 1991.[lxxvii] Shortly after, RSADSI CEO Jim Bidzos and Bill Gates held an all-day event strategising how to topple the encryption regulations.[lxxviii] Gates directed Bidzos towards a number of lobbyists who had good access to Clinton's inner circle.[lxxix] By the mid-1990s, Bidzos was also calling on

the lobbyist networks of RSADSI's licensees, who were all dependent on the liberalisation of cryptographic regulations to enable their global growth.[lxxx]

Influential Reports

One of the most influential industry lobbying groups was the Software Publisher's Alliance (SPA), which represented more than a thousand companies. In June 1993, the SPA published research arguing that the export controls had caused the US to lose its encryption market supremacy.[lxxxi] The SPA found that strong encryption was available outside the US, with 143 foreign encryption products on the global market (compared to 133 US products). The SPA study identified that at least 48 of those were using DES, and that 15 were described as 'mass market encryption software programs.'[lxxxii] The report noted that both PGP and DES were widely available on the internet.

In May 1997, the industry-funded Center for Democracy and Technology (CDT) coordinated a study of key-escrow's technical viability - *The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption*. The report stated that key-escrow:

> Will result in substantial sacrifices in security and greatly increased costs to the end-user. Building the secure computer-communication infrastructures necessary to provide adequate technological underpinnings demanded by these requirements would be enormously complex and is far beyond the experience and current competency of the field.[lxxxiii]

Government Incentives

The White House formally announced a modified version of the key-escrow policy on 12th July 1996.[lxxxiv] Now, 'trusted private sector parties' would hold the recovery keys, with a mechanism also in place for individuals and corporations to recover their own keys when required.[lxxxv] The administration stated that the approach would 'permit nations to establish an internationally interoperable key management infrastructure with rules for

access appropriate to each country's needs and consistent with law enforcement agreements.' The government would work with industry to develop appropriate standards for key recovery systems, allowing them to gain export permission. Notable in the press release was the favouring of the term 'key-recovery' rather than 'key-escrow'. Should industry agree to retain the keys instead of Federal agencies, this could instantiate trust in the key-escrow policy by introducing an additional barrier against Federal agents abusing the system.

In October 1996, Gore offered an incentive for industry to cooperate with key-recovery: 56-bit encryption, such as DES, would be exportable after a one-time government review of the product, and 'contingent upon industry commitments to build and market future products that support key recovery'. This accommodation was to last two years, after which only escrowed encryption over 40 bits would be exportable.[lxxxvi] This 56-bit encryption was a significant upgrade from the 40-bit restriction then in place on exportable cryptography. However, export licenses would only be granted for six-month periods - if a company failed to demonstrate developmental progress towards key-recovery, they could lose their license.[lxxxvii] In October 1996, eleven companies, including Apple, DEC, HP, IBM, and RSA, formed the 'key-recovery alliance' to 'develop an exportable, worldwide approach to strong encryption'.[lxxxviii].[lxxxix] Jim Bidzos, now part of the alliance, commented that 'in an imperfect world this technique will at least allow you to take advantage of what governments around the world will allow.'[xc] The alliance grew to more than fifty companies.[xci] Heidi Kukis from the Vice President's office commented 'I think we have a critical mass of companies willing to work with us.'[xcii]

International Community Reaction

Industry's argument rested on the international market's refusal to tolerate escrowed encryption. In the OECD, France sided with America's key-escrow proposals, whilst Australia, Canada, Denmark, and Finland all opposed on civil liberties grounds.[xciii] The UK initially sided with the US, but the new Labour government that took office in 1997 demurred.[xciv] An OECD policy paper of May 1997, representing the views of the broader 29 country members, did not support key-escrow.[xcv] The European Commission was explicit in rejecting key-escrow in October 1997, arguing that key-escrow could undermine digital commerce and internet adoption: 'If citizens and companies have to fear that their communication and transactions are monitored with the help of key access or similar schemes, they may prefer remaining in the anonymous off-line world.'[xcvi]

Results

Having reviewed the four main policy challenges that have been suggested as contributors to the discontinuance of the key-escrow policy, we now analyse the interviewee responses to assess their relative influence and impact.

The Advancement of Public Cryptography Knowledge

This advancement is perhaps best captured by the emergence of PGP. While PGP had the potential to grow into a technology that could undermine government mass-surveillance, in the 1990s its use remained niche. One of PGP's main challenges was that, in Bruce Schneier's words 'it lived and died on [its] usability.'[xcvii] Dorothy Denning, a professor of Computer Science and FBI advisor, reflects that PGP 'was just way, way too hard for the average person to use'. Schneier agrees, as does Electronic Frontier Foundation Co-Founder Mitch Kapor, who recalls that the software 'was impossibly difficult to use […] [you] had to be a technical expert to use PGP'.[xcviii] This poor user experience was critical to its uptake, and thus diminished the threat it posed to the key-escrow policy.

Richard George, former NSA Information Assurance Technical Director, reflects that 'the private cryptographer world had more of an influence on the technical people in government […] than it did on the policy makers.'[xcix] Kapor holds a similar belief: 'I doubt they [policy makers] even knew about it […] in general people in government and policy makers had no idea what was going on until it was too late to do anything about it.'[c] Bruce McConnell, Co-Chair of President Clinton's Inter-agency Committee on Encryption, comments that within policy circles PGP was 'a secondary argument, it was […] background noise'. McConnell reflects the view was that non-corporate developed technologies were 'unlikely to gain a major commercial foothold.' McConnell adds that 'the threat to intelligence community capabilities came much more from commercial

products.'[ci] The NSA likely assessed that any privately developed non-corporate cryptography would have vulnerabilities they were able to exploit. Stewart Baker, comments that his agency recognised that 'criminals and terrorists, and Phil Zimmermann, will all be able to write their own crypto', but he did not believe the NSA was concerned:

> If they [the NSA] could have guaranteed that no company that made more than $10 million a year ever tried to write a crypto program, they would have taken that deal, because they believed that anybody, any small company that tried to write a crypto program, would make mistakes that were exploitable.

PGP, they believed 'was not widespread, and so no-one thought that it was going to become a dangerous product by itself, but it was the beginning.'[cii] Jim Bidzos believed the same of non-corporately developed cryptography:

> The code was flawed in many cases, there were small bugs that could be exploited. And I know for a fact that […] there was some component of the folks in the government who thought just let it all go, let them do what they want, because they'll never get it right, they'll always be something to be exploited.[ciii]

Judging the impact of PGP on the key-escrow policy, Denning argues that it had, 'no impact at all', as the software was not mainstream, and was being used mostly by 'private individuals wanting to do their own thing.'[civ] Jim Dempsey, Vice President for Public Policy, Center for Democracy and Technology, reflects that any influence PGP may have had on the executive would have paled in comparison to the political clout of Microsoft and broader industry.[cv]

The growing public knowledge of cryptography, and industry's continuing sponsorship of interest groups such as the SPA, also led to an increase in the public's ability to scrutinize the technical viability of key-escrow. The paper, *The Risks of Key Recovery,*

Key Escrow, and Trusted Third-Party Encryption, embodied this ability. Douglas Miller, SPA's then lead for Government Affairs, recalls:

> We were eager to make the point that […] the genie is out of the bottle. There were already software programmes around the world that had encryption capabilities stronger than what the American export control limitations were, and so it [the encryption regulations] just simply had no national security benefit and [was] only a commercial disadvantage to American companies.[cvi]

Dempsey comments:

> You had the inventors of modern public key cryptography saying put aside the freedom versus security debate, put aside any civil liberties concerns - will this [key-escrow] work? And they said no, it will introduce some vulnerability that's unnecessary and basically will deny governments and business and individuals the benefits of the breakthroughs in cryptography.[cvii]

Dempsey states that the report 'stopped the government from saying we know what we're doing. Trust us.'[cviii] There was also a growing recognition that the spread of cryptographic knowledge was ultimately making the control of associated technologies increasingly impractical. Kapor reflects that 'you can't fight the forces of […] history […] crypto was going to happen […] people on the inside realized this was not a battle worth fighting […] because they were not going to succeed'.[cix]

Constitutional Challenges

The Bernstein, Karn, and Junger cases accentuated the potential constitutional issues existing with the legislation that hindered the free circulation of cryptographic knowledge and technologies.

Judge Patel's elevation of cryptographic code to speech established a precedent, one that could in the future be used for further challenges against the cryptography regulations, and in opposition to any key-escrow legislation. However, it was a ruling from a singular lower court that could not only be deviated from by peer judges, but overruled by higher

courts. The ruling, if it held, would perhaps mean the start of the end of encryption regulations that had stood sentry at US borders for a generation. Without such a barrier at the nation's perimeter, it would not be possible to stop the spread of cryptography such as PGP and its more powerful successors to other countries, meaning the establishment of a globally hegemonic US key-escrow norm would unlikely be achievable.

The difference between the Bernstein and Karn judgements in disparate parts of the country highlighted the growing divisions in cryptography policy. Karn's case was dismissed from a Washington court in the most unequivocal manner. Perhaps the judicial contrast was influenced by the geographies; Californian Judge Patel sat at the heart of the technology industry, whilst Judge Richey presided over a court in Washington D.C., the nexus of the government security apparatus. Richey's ruling would have given the Clinton administration hope that the cryptography regulations could be successfully defended in court, despite Patel's ruling. Yet, with the Judgement in favour of Junger, the government's position looked increasingly fragile.

It is not clear how much policy makers were aware of, or discussing, these three cases. Bruce McConnell recounts that 'In inter-agency briefs, and in the policy documents that we sent forward, which were all […] reviewed by the Justice Department, to the seniors and to the President, there was never mention of these cases as material to the [key-escrow] policy discussions.'[cx] This may have been because the Justice Department, with the FBI as a constituent entity, did not want the administration to be aware of the legal challenges, as it may have caused policy makers to withdraw their sponsorship of the key-escrow initiative it was championing. It could also have been as the government lawyers did not assess the rulings as a challenge to their ambitions. Dorothy Denning believes the

legal rulings were not a 'big factor' in the Clinton administration's decision to discontinue key-escrow.[cxi] Schneier goes further, arguing that the rulings did not have any 'direct effect […] at all.'[cxii]

In contrast, Marc Rotenberg, President of the Electronic Privacy Information' Center (EPIC), believes the decisions were influential. NSA's Richard George assesses that the court rulings were the 'main driver' in the key-escrow policy's discontinuation - he argues that the rulings brought the policy 'to its knees'.[cxiii] However, George believes that it was not the court rulings in isolation that were the determinant factor for key-escrow's discontinuation, but the broader privacy protestations: 'The key issue was just that the country was up in arms about the privacy issue and I think that the Clinton administration believed that, you know, it's just not going to work when we have that much of the country against it.'[cxiv] The NSA's General Counsel, Stewart Baker, also feels that the digital rights groups and the legal cases were influential in key-escrow's discontinuation, however not decisively so. Baker comments: 'you could get a bunch of lefties [digital rights groups] and academics to fight over key-escrow as a privacy issue, but I'm not sure that would have carried the day.'[cxv] Instead, Baker assesses that it was the impact of the digital rights groups in combination with industry's foreign market access concerns that resulted in key-escrow's discontinuation. Baker comments that 'Silicon Valley plus the privacy community usually wins, or at least is a very formidable force, and civil society privacy groups without industry aren't as anywhere near as formidable.'[cxvi]

Domestic Legislative Misalignment

Congress were exposed to a wide variety of views through the numerous hearings occurring throughout the 1990s, yet Jim Dempsey recounts within Congress there was a 'large middle that wasn't really deeply engaged in the issue one way or another and didn't claim to understand the issues'. Dempsey identifies smaller government-security-law enforcement, and libertarian-civil liberties-technology contingents that were in conflict over the key-escrow policy. Dempsey observes the 'curious factor' that some of the strongest supporters of industry were from rural areas, 'they saw it as giving their citizens access to information that they had previously been denied because of the constraints of distance'.[cxvii]

Increasingly it was economic factors that drove Congressional thinking, yet the security lobby remained powerful. Throughout most of the 1990s there was no congressional consensus on cryptography policy due to these competing interests. This is evidenced by numerous cryptography-related bills introduced in Congress, often in a strike-counter-strike pattern. Most of these bills were positioned at either end of the spectrum (i.e., heavily regulating encryption, or withdrawing nearly all regulations) - few had any prospect of success. Such proposed legislation included the:

- Anti-Electronic Racketeering Act (1995)
- Encrypted Communications Privacy Act (1996)
- Promotion of Commerce On-Line in the Digital Era (PRO-CODE) Act of 1996
- Safety and Freedom Through Encryption (SAFE) Act (1997)

None of these bills became law. The interviewee's responses did not highlight the legislative challenges as being a determinant factor or major contributor in the failure of the policy.

Industry's Foreign Market Access

McConnell reflects that 'Industry was very effective in Congress in terms of building political support […] for the de-emphasis of key-recovery.'[cxviii] Baker observes that Microsoft drove the effort, conducting 'most of their lobbying through […] trade associations that they dominated […] They were very supportive of the [digital] civil liberties groups, and there's a long history of tech companies supporting the civil liberties society lobby for their own business purposes'.[cxix] Baker comments that 'Microsoft had a lot of money and a lot of clout […] it could determine the direction of most of the lobbying that occurred through trade associations.' Dempsey comments that 'Microsoft and others were able to make the argument that […] American products are not going to be [globally] viable […] because our products won't be trusted. Whether that argument was true or not it […] became an almost immovable object.'[cxx] Baker reflects that 'nobody looked too closely' at this argument postulated by industry. Baker continues:

> Maybe it [key-escrow] could have been made commercially acceptable. You just say, well, key-escrow we sold it in Turkey, and we escrow the keys in Turkey, and if you use a Turkish product you're subject to Turkish court orders - you could have come up with something. But nobody wanted to do that, and they just said it won't work, and who was going to say that it would work? Nobody relies on [the] NSA for market studies, so that was probably the kiss of death.[cxxi]

Microsoft's most visible ally, RSADSI's Jim Bidzos was also driving the regulatory liberalization effort by employing his network's lobbying prowess. He reflects: 'I think that [they] really made the difference.'[cxxii] In late 1997, Bidzos also met the Clintons at a

Democratic fundraising event in California where the former was able to further petition for regulatory liberalization. Bidzos reflects that Clinton understood the 'argument of inevitability' and was 'very well informed.' Bidzos recalled that Clinton said 'I feel your pain […] I think you have the better argument, but you have to understand that I've got the heads of the CIA, the NSA and the FBI, all telling me to be very careful, because this is an important issue.' Bidzos comments 'Clinton understood [that] all you're [the administration is] doing is you're going to negatively impact this huge wave of economic growth that the country is experiencing, driven by tech.'[cxxiii]

The CRISIS report had advised that the government should respect the 'legitimate national needs of law enforcement and intelligence […] to the extent consistent with good information protection.'[cxxiv] The subtext of this advice could be interpreted as implying that key-escrow was not consistent with good information protection, and therefore need not be respected. The OECD report was particularly influential in Washington DC according to Jim Dempsey and Marc Rotenberg.[cxxv] Rotenberg assessed that the 'US proposal to endorse lawful access to private keys was explicitly rejected by the OECD,' and that the organisation had instead chosen a policy, 'based on voluntary, market-driven development of cryptography products.'[cxxvi] Dempsey and Rotenberg both feel that the OECD principles, which did not explicitly support escrowed encryption, were particularly influential in the US decision to discontinue its key-escrow policy.[cxxvii] With the EU also moving away from key-escrow, any hope for an interconnected global system of national key-escrow systems was lost. If US companies could only sell escrowed encryption systems, even close allies would likely be resistant to acquiring technology that enabled the US government to have potentially pervasive access to their communications. Rotenberg further believes the CRISIS report `was very influential in

Washington because it was viewed as an authoritative, independent assessment.'[cxxviii] By this point, Rotenberg believes 'The government's [key-escrow] campaign was running out of steam.'[cxxix] The CRISIS and PECSENC reports had also increased the evidence that encryption controls were decreasing US prosperity, and that strong encryption systems were already proliferating globally.

As the policy struggled to gain public acceptance, McConnell recalls that the Clinton administration:

> morph[ed] the policy from key-escrow to key-recovery, and marketed it, then as the thing that everybody will want because people are going to lose their [encryption] keys. And so they're going to want the provider to be able to recover their plaintext, etc. And so we need to have key-recovery, and its just a matter of who holds the keys.[cxxx]

Whilst large swathes of industry, in principle, subsequently agreed to develop key-recovery solutions when offered immediate export concessions, the intent to deliver on this agreement was ambiguous. Despite their words and actions, it is unknown whether the commercial organisations truly intended to support key-recovery. For instance, the lack of Bidzos' complete fidelity to the key-recovery alliance was in evidence in September 1997, when in a *New York Times* article he wrote 'Contrary to the position of the FBI […] the proposal for key-recovery is not the digital equivalent of putting alligator clips on phone wires. It's more like giving the government the keys to all of our personal and professional lives.'[cxxxi] Clearly, despite the formation of the key-recovery alliance, Bidzos was not intent on withdrawing his protestations against government encryption policies. Whilst Bidzos' recollection of this period is incomplete, he comments that the key-recovery alliance was 'just one of the many attempts to do something more balanced.' Bidzos adds 'I never took the position that we don't want to talk to you [the Clinton administration] because key-recovery is a bad term, or government access is a bad term;

I've always felt that the capability should be there.' Of the other members of the alliance, Bidzos comments that 'Some of them just wanted to basically not rebuff a government proposal, they didn't want to just say no - some of them wanted to genuinely help.'[cxxxii]

By late 1997, Bruce McConnell comments that 'the general feeling' in government was that 'The horses [are] out of the barn and so why are we trying to hold back American industry?' McConnell believes that 'industry was the strongest voice and the biggest factor' in the discontinuance of key-escrow. McConnell comments of industry:

> they were very effective in making the case that […] people will buy it [encryption] from other countries and so therefore, we'll have less visibility into what's going on […] this will hurt American industry […] the privacy […] arguments were made, but the industry arguments […] could be heard more easily by the interagency [working group on encryption].[cxxxiii]

Likewise, Dorothy Denning assesses that 'Industry played […] maybe the highest role [in the decision to discontinue Clipper].'[cxxxiv] Denning comments that 'Industry wanted export relief, not key-escrow. If the US didn't provide the crypto that the world demanded, other countries would.' Denning also believes that key-escrow's chances of success were impacted by the fact that, despite their narrative 'The FBI was not having all that much trouble dealing with crypto, which is what started the key-escrow effort in the first place.'[cxxxv] Whilst William Reinsch, the Under Secretary of Commerce for Export Administration, does not believe it was a singular variable that resulted in the key-escrow's discontinuation, he does believe that 'fierce industry resistance was an important factor. Everybody understood that it wouldn't work if the companies didn't want to make it work.' Reinsch comments:

> It was not that hard to make encryption products […] if other people were going to buy this product, it was better if they bought the American product than if they bought an Israeli product or a Russian product or a French product that we didn't know anything about. And now once you got it, it became easier for the government to make a decision about how to control the

> product. Although I have to say, the FBI director never understood, never.[cxxxvi]

Among the subjects interviewed there was only one dissenter with regards to the impact of industry on the debate, that of the NSA's Richard George, who comments 'I didn't see industry as being a big influencer.'[cxxxvii] However, whether George had an adequate vantage point from which to see industry's machinations from within NSA's information assurance directorate is unclear.

Discussion

Having examined each of the four challenges key-escrow confronted, the evidence suggests that it was primarily industry's objections to the policy that caused its demise. The chance of key-escrow being practical at a global level, across political, and ethical fault lines was fraught with likely unresolvable dilemmas. Given this reality, industry's apprehension that key-escrow would curtail its foreign market access, and the US's global technological dominance, was valid. When the OECD and EU failed to support key-escrow in late 1997, any hopes of a multi-national accord that could preserve industry's foreign market access, whilst satisfying the government's desire for surveillance capabilities, was lost. Most interviewees, including McConnell, whose role at the heart of the government's key-escrow strategy provides his account a great measure of credence, believes it was this loss of international market access that caused the key-escrow to lose its political viability.

Whilst PGP was recognised as a harbinger of the threat posed by open-source cryptography, one that would be realised in the twenty-first century, interviewees felt it had neither achieved the market penetration nor influenced decision-makers sufficiently to merit a challenge to the key-escrow policy. The broader proliferation of cryptography knowledge that allowed technical criticisms of the policy were believed to have been more impactful. Perhaps the most high-profile such criticism was made by AT&T's Matt Blaze.[cxxxviii] Whilst some, such as Brantly, and Riebe et al., have argued Blaze's research was responsible, or partly responsible, for key-escrow's demise, none of the interviewees raised this as the determinative factor.[cxxxix] In fact, Blaze had thanked NSA for their 'openness and collegiality' in reviewing his research, and had subsequently been trusted with assessing a prototype for *Tessera*, a next generation key-escrow device.[cxl] Further,

Blaze's research was released in 1994, and the key-escrow initiative was still active as late as 1997, suggesting either it was not the determinative reason for the policy's failure, or its consequences were severely delayed – however, this theory is not supported by interviewee responses. Technical criticisms were often purist arguments. Whilst this is not to say they were incorrect, the relevant question for policy makers was likely not whether key-escrow would create an additional weakness within the digital ecosystem, but whether the government was willing to accept that risk in exchange for the perceived gains with which they would be endowed against what may have been judged a broader spectrum of risks. Therefore, technical arguments probably only had at most a minor impact on the discontinuance of key-escrow.

The legal battles regarding the constitutionality were incomplete at the time of key-escrow's discontinuation, and given interviewees statements that the government's cryptography working group were not discussing these issues, it is unlikely this challenge that caused the policy's demise. That is not to argue that the rulings did not have the potential to be impactful, but there is no evidence that the senior leadership of the administration were concerned regarding the potential implications of these cases.

Interviewees placed little weight on the congressional impasse regarding key-escrow. It is unclear whether, had there been international consensus regarding key-escrow, Congress would have supported the policy, as claimed by Pednekar-Magal and Shields. Such consensus would not remedy the encryption regulation's constitutional deficiencies, nor reconcile whether key-escrow was compatible with Congress' conception of citizen's freedom and privacy rights. There was no certainty the SAFE bill would have succeeded, even with an international key-escrow treaty forged. Given the interviewees placed little

emphasis on Congressional challenges being the determinant cause of key-escrow's discontinuation, it is assessed that whilst Congress was an important theatre of debate, and would have become more so if an international key-escrow accord were agreed, industry's objections were more consequential in the policy's failure.

Consequences of Key-Escrow's Failure & The Enduring Crypto Wars

Rotenberg observes that key-escrow 'is one of those battles that […] doesn't necessarily stay won.'[cxli] Dempsey concurs: 'In politics there are very *very* few permanent victories. The issue was resolved for the time […] But none of these issues is ever *over* over.'[cxlii] Indeed, since key-escrow's discontinuation skirmishes have continually occurred as to the degree citizens should be permitted access to encryption technologies, and to broader digital privacy, lacking exceptional access provisions. Numerous government proposals have attempted to provide access to citizen's communications. For instance, UK government officials have suggested that, when required, service providers 'silently add' an additional (government) user to encrypted chats to facilitate access.[cxliii] In another example, to address the challenge of child sexual abuse material (CSAM), client-side scanning has been suggested, whereby the mathematical hash[1] of each image on a device/application is compared to a centralised CSAM library, with law enforcement notified of matches.[cxliv] These approaches were unsuccessful due to civil rights groups protesting, and companies objecting to the technical vulnerabilities such approaches would introduce, as well as the abuse risk.[cxlv]

[1] Hash functions are mathematical algorithms allowing a unique fixed string of characters (a hash) to be generated from an input file.

Overt attempts to defeat or circumvent encryption were paired with covert measures. These include PRISM, a capability revealed by former NSA contractor Edward Snowden in 2013.[cxlvi] Journalists Greenwald and MacAskill reported how the top secret PRISM program provided, 'direct access to the systems of Google, Facebook, Apple, and other US internet giants,' allowing data collection including, 'email, video and voice chat, videos, photos, voice-over-IP chats (e.g., Skype), file transfers, social networking details, and more.' [cxlvii] The authors alleged the complicity of the technology companies; Google and Apple denied involvement. NSA documents showed PRISM originated in 2007. A leaked document lauded PRISM as 'one of the most valuable, unique and productive accesses for NSA,' resulting in more than 77,000 intelligence reports.[cxlviii] Being able to access back-end technology systems with the cooperation/coercion of vendors likely would have removed the need to break encrypted data, or develop a key-escrow like capability requiring public consent.

Snowden also revealed NSA's Operation BULLRUN, described by Ball et al. as a UK/US capability that had 'successfully cracked much of the online encryption relied upon by hundreds of millions of people to protect the privacy of their personal data, online transactions, and emails.'[cxlix] Methods included, 'covert measures to ensure NSA control over setting of international encryption standards, the use of supercomputers to break encryption with "brute force," and […] collaboration with technology companies and internet service providers.' [cl] BULLRUN's initiation date is unknown; however, a 2010 GCHQ document stated, 'For the past decade, NSA has lead [sic] an aggressive, multi-pronged effort to break widely used internet encryption technologies,' placing its origins at the turn of the millennium. [cli] It is possible the NSA, and US government, recognised

they had lost the public battle for access to encrypted data during the debates of the 1990s, and consequently increased investment in covert access.

One of the primary BULLRUN projects was to 'actively engage US and foreign IT industries to covertly influence and/or overtly leverage their commercial products' designs,' and to 'insert vulnerabilities into commercial encryption systems.'[clii] The objective was to 'make the systems in question exploitable through SIGINT collection […] with foreknowledge of the modification. To the consumer and other adversaries, however, the systems' security remains intact.' [cliii] This description is reminiscent of key-escrow's goals. A significant example of this approach is the NSA's alleged sabotage of a pseudo random number generator [PRNG], critical to the integrity of an encryption algorithm within a prominent global standard.[cliv] In September 2013, The *New York Times* claimed it found data in the Snowden archives confirming NSA's role in manipulating the Dual_EC_DRBG algorithm (the raw Snowden / NSA files themselves were not released). The newspaper detailed how, 'Classified NSA memos appear to confirm that the fatal weakness, discovered […] in 2007, was engineered by the agency. The NSA wrote the standard and aggressively pushed it on the international group.'[clv] Dual_EC_DRBG was implemented as an optional PRNG in several products including Microsoft's SChannel (used in Internet Explorer and in widely used web server Internet Information Services [IIS]) and OpenSSL's FIPS module; RSA's BSAFE crypto libraries used Dual_EC_DRBG as a default PRNG.[clvi]

Fallout from the Snowden revelations likely re-emphasized to US companies that to maintain foreign market access they needed to demonstrate a degree of independence from the US government. This realization probably fuelled the public contestation

between the FBI and Apple when the former asked the latter to unlock an iPhone belonging to a domestic terrorist in 2016. The episode saw the parties end up in legal battle, the conclusion of which was prevented only by the FBI reportedly gaining access to the device through a third-party facilitating access using a technical vulnerability.[clvii] The episode suggested that at least some companies, likely fearing domestic and international public reaction, potentially to the detriment of their commercial interests, were no longer complying with government requests.

The key-escrow policy was an early indication of how significant technology companies would become in the formulation and execution of surveillance policy in the twenty-first century. Rozenshtein observes these 'surveillance intermediaries' have 'financial and ideological incentives to resist government requests for user data'.[clviii] Rozenshtein argues such intermediaries use three 'categories of resistance': *Proceduralism*: a refusal to cooperate with governments outside of formal process whilst exhibiting a willingness to challenge government requests in course; *Technological unilateralism*: architectural product modifications to stymie the company's technical ability to help the government, such as the use of end-to-end encryption, and to further the challenge of authorities independently finding a technical vulnerability in the product enabling subversion of its protections; *Policy mobilization*: Using social and political influence, in combination with disclosure of government surveillance requests, to change associates policies. Apple exhibited all of these in its contest with the FBI. Rozenshtein further contends that intermediaries 'contribute by adding more information about surveillance costs and by incentivizing the government to limit nonessential surveillance,' yet their role challenges 'the state's monopoly over security, the very locus of traditional conceptions of sovereignty'.[clix] Rozenshtein concludes that understanding how technology companies

wield this power, and whether it is 'legitimate and desirable will be one of the key projects for […] law and legal scholarship as society pushes ever more completely into the digital age'.[clx]

Dempsey highlights one important difference between today and the 1990s, when he comments 'We are in a way right back where we were, with the exception of course that the inertia is currently in favour of industry, whereas the inertia […] in the 1990s, meant [that] limits would remain on encryption […] [which] favoured the government.'[clxi] Baker agrees stating that 'Right now it looks as though the debate over warrant-proof encryption is still moving in the direction of, or is still stuck at a status quo, that is very favorable to warrant-proof encryption.'[clxii] However, Baker warns:

> we [the NSA] were right. The criminal misuse, the terrorist misuse, of really strong encryption is here and we are just beginning to truly feel the earliest fruits of mass-market unbreakable [encryption] […] and as those consequences become clear, the debate continues, because it's one thing to stand for privacy in the abstract, and believe in civil liberties in the abstract, and it's another thing to live with the consequences of truly guaranteeing the privacy of every human being on the planet. We're going to see some unhappy consequences, […] some very unhappy consequences.[clxiii]

Today, society is dependent on technology in ways that would have been inconceivable to all but the most prescient during the 1990s. Encryption now protects our satellites, hospitals, economies, and even communications to devices implanted within our citizens, such as pacemakers. Rotenberg expands on the changing need for encryption since the 1990s:

> There are real world consequences of subverting a secure communications channel that go far beyond gaining access to someone's private email or their credit card number, which is what we were about in the early 1990s, so it would be very dangerous […] today for government to propose weakened or key-escrowed encryptions.[clxiv]

But equally, one could argue that the threats have also increased. As our societies have digitised, so have a plethora of malicious actors exacerbating risk to all parties.

Governments today might make the argument that if the internet is in fact the new town square, as well as the new interstate highway and the new foundation upon which prosperity depends, then it would be in dereliction of duty to not afford it suitable protection, which would necessitate surveillance. This debate will undoubtedly continue into the future.

Conclusion

This article has examined the determinant reason for the discontinuance of the key-escrow policy. Pednekar-Magal and Shield's 2003 research found that intra-government conflicts between the executive and Congress may have played an important role in the failure of the key-escrow policy. However, this study has argued that the availability of further source material now suggests that industry concerns were most likely the determinant reason for the discontinuance of the key-escrow policy. Our analysis suggests that the advancement of public cryptography knowledge, judicial rulings against the constitutionality of cryptographic regulations, and congressional inertia contributed to a significantly lesser degree.

Appendix A) Interview Subjects

Interviewee	Relevant Former Positions
Stewart Baker	General Counsel, NSA (1992-1994).
Jim Bidzos	President and CEO RSADSI, Public Key Partners, and VeriSign (1990s).
Jim Dempsey	Assistant Counsel, House Judiciary Committee, Subcommittee on Civil and Constitutional Rights (1985-1995); Deputy Director, Center for National Security Studies (1995-1997); Senior Counsel, Deputy Director, Executive Director, Vice President for Public Policy, Center for Democracy and Technology (1997-2014).
Professor Dorothy Denning	FBI Advisor; High-profile Clipper advocate; Chair of Computer Science at Georgetown University.
Richard George	Information Assurance Directorate Technical Director, NSA (197x-2011).
Mitch Kapor	Co-founder, Electronic Frontier Foundation (EFF).
Bruce W. McConnell	Co-Chair, President Clinton's Inter-agency Committee on Encryption (1993-1997); Chief, Information Policy and Technology, Office of Management and Budget (1986-1999).
Douglas Miller	Government Affairs, Software Publisher's Association (SPA) (1990s).
William Alan Reinsch	US Under Secretary of Commerce for Export Administration, Clinton Administration.
Marc Rotenberg	Washington Director, Computer Professionals for Social Responsibility (CPSR) (1988-1994); Co-founder and President, Electronic Privacy Information Center (EPIC) (1994-2020).
Bruce Schneier	Cryptographer, EFF & EPIC Board member; Public Policy Lecturer and Harvard University Fellow.

Appendix B) Interview Schedule

	Question
1	Were you involved in the key-escrow policy?
1a	Can you recount the evolution of the key-escrow policy and your role within the policy?
1b	Do you feel there was a specific point when the key-escrow policy was discontinued by the Clinton administration?
1c	If so, when do you feel this decision was taken?
1d	What do you assess was the determinant reason the key-escrow policy was discontinued?
1e	To what degree do you assess industry influenced the evolution of the key-escrow policy?
1f	To what degree do you assess industry influenced the discontinuation of the key-escrow policy?
1g	To what degree do you assess private cryptographers and their inventions, such as Phillip Zimmermann and his PGP software, influenced the evolution of the key-escrow policy?
1h	To what degree do you assess private cryptographers influenced the discontinuation of the key-escrow policy?
1i	To what degree do you assess digital civil rights groups launching legal challenges against cryptographic regulations, and the subsequent judicial ruling that cryptographic source code was constitutionally protected speech, influenced the evolution of the key-escrow policy?
1j	To what degree do you assess digital civil rights groups launching legal challenges against cryptographic regulations, and the subsequent judicial ruling that cryptographic source code was constitutionally protected speech, influenced the discontinuation of the key-escrow policy?
2	Is there anything else about the key-escrow policy you would like to share that you feel pertinent to this research?
3	Is there anything else regarding the wider 1990s crypto wars you would like to share that you feel is pertinent to this research?
4	What do you think is the legacy of the key-escrow policy?
5	Do you think key-escrow could happen today?

Acknowledgments

The authors would like to thank the three anonymous reviewers of this article whose insights greatly improved the final submission.

Declaration of Interest Statement

The authors have no competing interests to declare.

Bibliography

Abelson, Hal, Ross Anderson, Steven M Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, et al. “The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption” 27 May, 1997. https://web.archive.org/web/20210125182103/http://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/key-study-report.html.

Advanced Telephony Unit, Federal Bureau of Investigation. “Impact of Emerging Telecommunications Technology on Law Enforcement” Columbia University, 1992. https://web.archive.org/web/20200716170720/https://www.cs.columbia.edu/~smb/Telecommunications_Overview_1992.pdf.

Aldrich, Richard J. *GCHQ: The Uncensored Story of Britain’s Most Secret Intelligence Agency*. London: Harper Press, 2019

Andrews, Edmund L “Europeans Reject U.S. Plan On Electronic Cryptography” *The New York Times*, 9 October, 1997. https://web.archive.org/web/20190713223119/https://www.nytimes.com/1997/10/09/business/international-business-europeans-reject-us-plan-on-electronic-cryptography.html.

Apple, Atalla and others. “Joint Press Announcement: High-Tech Leaders Join Forces to Enable International Strong Encryption” 1996. https://web.archive.org/web/20201205183447/https://www.epic.org/crypto/key_escrow/joint_announce_10_2_96.html.

Baker, Stewart, interview by Craig Jarvis. 2021.

Banisar, David. “Stopping Science: The Case of Cryptography” *Health Matrix: The Journal of Law-Medicine 9,* no. 2 (1999): 253-287.

Barlow, John Perry. “Jackboots on the Infobahn” 1 January, 1994. https://web.archive.org/web/20201206184415/https://www.wired.com/1994/04/privacy-barlow/.

Bass, Kenneth, Frank W. Hunger, Eric H. Holder, Vincent M. Garvey, and Anthony J. Coppolino. “Stipulation and Proposed Scheduling Order” QualComm, 1997. https://web.archive.org/web/19990128172006/http://people.qualcomm.com/karn/export/stip.html.

Bauman, Zygmunt, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, and R. B. J. Walker. “After Snowden: Rethinking the Impact of Surveillance” *International Political Sociology* 8 (2014): 121-144.

Bernstein, Daniel. “Curriculum Vitae” 2008. https://web.archive.org/web/20201004054738/https://cr.yp.to/cv/cv-20080915.pdf.

Bernstein, Daniel. “Declaration of Daniel J. Bernstein: Daniel J. Bernstein Vs United States Department of State et al.” 1996. https://web.archive.org/web/20200502055903/https://cr.yp.to/export/1996/0726-bernstein.txt.

Bidzos, Jim, interview by Craig Jarvis. 2021.

Bidzos, Jim. “Nothing Safe About Encryption Bills” *The New York Times*, 26 September, 1997: A26.

Blaze, Matt. “Key Escrow from a Safe Distance: Looking Back at the Clipper Chip” 2011. https://web.archive.org/web/20220327020933/https://www.mattblaze.org/escrow-acsac11.pdf.

Bidzos, Jim. “Protocol Failure in the Escrowed Encryption Standard” 20 August, 1994. https://web.archive.org/web/20230821220843/https://www.mattblaze.org/papers/eespro to.pdf.

Brantly, A. F. “Banning Encryption to Stop Terrorists: A Worse than Futile Exercise” 2017. https://web.archive.org/web/20221127153356/https://ctc.westpoint.edu/wp-content/uploads/2017/08/CTC-Sentinel_Vol10Iss7-10.pdf.

Bryman, Alan. *Social Research Methods.* Oxford: Oxford University Press, 2016.

Burns, Conrad. “Open Letter to the internet Community” 1996. https://web.archive.org/web/20201204190709/https://www.epic.org/crypto/legislation/burns_letter.html.

Butler, James R., and Karen A. Forcht. “The Clipper Chip and the Price of Security in America” *Information Management & Computer Security* 1 no. 5 (1994): 9-12.

Clinton, Bill. “Address by President Bill Clinton to the UN General Assembly: September 27, 1993” 1993. https://web.archive.org/web/20210113104012/https://2009-2017.state.gov/p/io/potusunga/207375.htm.

Clinton, Bill. “Statement on Signing the Telecommunications Act of 1996” The White House, 1996. https://web.archive.org/web/20210307111805/https://www.govinfo.gov/content/pkg/PPP-1996-book1/html/PPP-1996-book1-doc-pg188.htm.

Cohn, Cindy A. “Daniel J. Bernstein Vs United States Department of State et al.” 1995. https://web.archive.org/web/20170827104411/https://cr.yp.to/export/1995/0221-cohn.txt.

Dempsey, Jim, interview by Craig Jarvis. 2021.

Denning, Dorothy, interview by Craig Jarvis. 2021.

Electronic Frontier Foundation. “EFF Sues to Overturn Cryptography Restrictions” 1995. https://web.archive.org/web/20200813163721/https://www.eff.org/press/archives/2008/04/21-42.

Esposti, Sara Degli, and Elvira Santiago-Gomez. “Acceptable Surveillance - Orientated Security Technologies: Insights from the SurPRISE Project” *Surveillance & Society* 13, no. 3/4 (2015): 437-454.

Froomkin, Michael A. “The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution” *University of Pennsylvania Law Review* 13, no. 3 (1995): 709-897.

George, Richard, interview by Craig Jarvis. 2021.

Gonzalez-Barahona, Jesus M. “A Brief History of Free, Open Source Software and Its Communities” IEEE Computer Society, 2021. https://web.archive.org/web/20210427073256/https://ieeexplore.ieee.org/ielx7/2/9353489/09353517.pdf.

Greenwald, Glenn. “NSA collecting phone records of millions of Verizon customers daily” *The Guardian,* 6 June, 2013. https://web.archive.org/web/20230919170744/https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

Greenwald, Glenn, and Ewen MacAskill. “NSA Prism program taps in to user data of Apple, Google and others” *The Guardian,* 6 June, 2013. https://web.archive.org/web/20130801183931/https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

Hughes, Sunny Skye. “US Domestic Surveillance after 9/11: An Analysis of the Chilling Effect on First Amendment Rights in Cases Filed against the Terrorist Surveillance Program.” *Canadian Journal of Law and Society* 27, no. 3 (2012): 399-425.

Jarvis, Craig. *Crypto Wars: A Political History of Digital Encryption*. London: CRC Press, 2020.

Jarvis, Craig. “What caused the Clinton administration to discontinue its efforts to regulate digital cryptography via surveillance technologies implanted in consumer products, 1993-1998?” PhD diss. Royal Holloway, University of London, 2021. https://web.archive.org/web/20230918161405/https://pure.royalholloway.ac.uk/ws/portalfiles/portal/43934050/2021JarvisCPhD.pdf.

Junger, Peter. “Declaration of Peter Junger” 1996. https://web.archive.org/web/19970318220518/http://www.eff.org/pub/Privacy/ITAR_export/Junger_v_DoS/junger.declaration.

Kapor, Mitch, interview by Craig Jarvis. 2021.

Lash, Alex. “Computer Alliance Supports Encryption Policy” 1996. https://web.archive.org/web/19970605171214/http://www.news.com/News/Item/0,4,4063,00.html.

Levy, Ian, and Crispin Robinson. “Principles for a More Informed Exceptional Access Debate” 29 November, 2018. https://web.archive.org/web/20220419012557/https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate.

Levy, Ian, and Crispin Robinson. “Thoughts on Child Safety on Commodity Platforms” 21 July, 2022. https://web.archive.org/web/20230709011343/https://arxiv.org/pdf/2207.09506.pdf.

Markoff, John. “Data-Secrecy Export Case Dropped by I.S.” 12 January, 1996. https://web.archive.org/web/20201119112524/https://www.nytimes.com/1996/01/12/business/data-secrecy-export-case-dropped-by-us.html.

Markoff, John. “U.S. Rebuffed in Global Proposal For Eavesdropping on the internet.” *New York Times*, 27 March, 1997. https://web.archive.org/web/20171229173815/https://www.nytimes.com/1997/03/27/business/us-rebuffed-in-global-proposal-for-eavesdropping-on-the-internet.html.

Martin, Keith. *Cryptography: The Key to Digital Security, How It Works, and Why It Matters*. New York: WW Norton & Co, 2021.

McConnell, Bruce, interview by Craig Jarvis. 2021.

McCurley, Kevin. “History of the IACR.” No date. Accessed March 21, 2023. https://web.archive.org/web/20220305154524/https://iacr.org/docs/history/.

Miller, Douglas, interview by Craig Jarvis. 2021.

Mulivor, Phil. “SPA Press Release (MessageID: ‘9306061624.AA09694@relay2.UU.NET’)” 4 June, 1993. https://lists.cpunks.org/pipermail/cypherpunks/2013-September/000741.html.

National Research Council. *Cryptography's Role in Securing the Information Society*. Washington, DC: The National Academies Press, 1996.

Open Rights Group. “Online Safety Bill: Civil society organisations urge UK to protect global digital security and safeguard private communication” 26 June, 2023. https://web.archive.org/web/20230629171452/https://www.openrightsgroup.org/publications/open-letter-protect-encrypted-messaging/.

Organisation for Economic Co-operation and Development. “Recommendation of the Council Concerning Guidelines for Cryptography Policy” 1997. https://web.archive.org/web/20210327115602/https://one.oecd.org/document/C%2897%2962/FINAL/en/pdf.

Pednekar-Magal, Vandana, and Peter Shields. “The State and Telecom Surveillance Policy: The Clipper Chip Initiative.” *Communication Law and Policy* 8, no. 4 (2003): 429-464.

Portnoy, Erica. “Why Adding Client-Side Scanning Breaks End-To-End Encryption” 1 November, 2019. https://web.archive.org/web/20230919202823/https://www.eff.org/deeplinks/2019/11/why-adding-client-side-scanning-breaks-end-end-encryption.

President's Export Council Subcommittee on Encryption. “Findings of the President’s Export Council Subcommittee on Encryption” 18 September, 1998. https://web.archive.org/web/20210330171224/https://www.govinfo.gov/content/pkg/CHRG-106shrg69984/pdf/CHRG-106shrg69984.pdf.

Reinsch, William, interview by Craig Jarvis. 2021.

Richey, Charles R. “Memorandum Opinion of Charles R. Richey, United States District Court Judge” 1996. https://web.archive.org/web/20000817000154/http://people.qualcomm.com/karn/export/richey_decision.html.

Riebe, Thea, Phillipp Kühn, Philipp Imperatori, and Christian Reuter. “U.S. Security Policy: The Dual-Use Regulation of Cryptography and its Effects on Surveillance” *European Journal for Security Research* 7 (2022): 39-65.

Rotenberg, Marc, interview by Craig Jarvis. 2021.

Rozenshtein, Alan Z. “Surveillance Intermediaries” *Stanford Law Review* 70 no. 99 (2018): 99-189.

Scarselli, Gino. “Correspondence to the Department of Commerce, June 12, 1997” 12 June, 1997. https://web.archive.org/web/20060912162558/http://samsara.cwru.edu/comp_law/jvd/pdj-bxa-gjs080797.html.

Schneier, Bruce, interview by Craig Jarvis. 2021.

Schneier, Bruce. *Applied Cryptography Protocols, Algorithms, and Source Code in C.* New York: John Wiley and Sons, 1993.

Steinert-Threlkeld, Tom. “Cryptography tests rights of electronic word” *Dallas Morning News.* 23 July, 1994.

Strasheim, Alex. “Re: Zimmermann case is dropped; MessageID: ‘199601120205.UAA02271@proust.suba.com'” 11 January, 1996. https://lists.cpunks.org/pipermail/cypherpunks/2013-September/000741.html.

The White House. “Administration Statement on Commercial Encryption Policy, 12 July 1996” 1996. https://web.archive.org/web/20201125212614/https://www.epic.org/crypto/key_escrow/wh_cke_796.html.

The White House. “Executive Order 13026 of November 15, 1996: Administration of Export Controls on Encryption Products” 1996.

https://web.archive.org/web/20201112022645/https://www.govinfo.gov/content/pkg/FR-1996-11-19/pdf/96-29692.pdf.

United States Attorney. “US DoJ Zimmermann Press Release” Cypherpunk Mail List Archives 1992-1998. 12 January 1996. https://lists.cpunks.org/pipermail/cypherpunks/2013-September/000741.html.

United States Congress. “S.266 - Comprehensive Counter-Terrorism Act of 1991” 1991. https://web.archive.org/web/20201101073051/https://www.congress.gov/bill/102nd-congress/senate-bill/266.

United States Congress. “S.974 - Anti-Electronic Racketeering Act of 1995” 1995. https://web.archive.org/web/20201213000729/https://www.congress.gov/bill/104th-congress/senate-bill/974.

United States Court of Appeals for the Ninth Circuit. “Order: Daniel J. Bernstein Vs United Department of State et al.” 1997. https://web.archive.org/web/20170827104309/https://cr.yp.to/export/1997/0922-order.txt.

United States Department of Commerce. “EAR: Enforcement and Protective Measures” 2001. https://web.archive.org/web/20170827104129/https://cr.yp.to/export/ear2001/764.pdf.

United States Department of Commerce. “Letter from Patricia Sefcik, Director of Encryption Policy Controls Division US Department of Commerce to Philip Karn, 20 November” 1997. https://web.archive.org/web/19990222025524/http://people.qualcomm.com/karn/export/bxa_license_denial.html.

United States Department of Justice. “Daniel J. Bernstein Vs United Department of State et al: Defendant’s Notice of Motion and Motion for a Stay Pending Appeal and to Shorten Time Ex Parte Motion” 1997. https://web.archive.org/web/20170827104259/https://cr.yp.to/export/1997/0827-coppolino.txt.

United States Department of State. “Request for Commodity Jurisdiction Determination for: Applied Cryptography Source Code Disk” 1994. https://web.archive.org/web/19990224102110/http://people.qualcomm.com/karn/export/floppy-cjr-response.html.

United States District Court for the Northern District of California. “Opinion: Daniel J. Bernstein Vs United States Department of State” 1997. https://web.archive.org/web/20170827104346/https://cr.yp.to/export/1997/0825-order.html.

United States District Court Northern District of California. “United States District Court Northern District of California Vs Daniel J. Bernstein: Opinion (MessageID:

199604190802.BAA11461)" April, 1996. https://lists.cpunks.org/pipermail/cypherpunks/2013-September/000741.html.

United States District Court Northern District of Ohio Eastern Division. "Preliminary Injunction: Judge Donald C. Nugent" 1996. https://web.archive.org/web/19970318220530/http://www.eff.org/pub/Privacy/ITAR_export/Junger_v_DoS/junger_injunction.draft.

United States House of Representatives. "Hearing on H.R. 695 Safety and Freedom Through Encryption (SAFE) - March 20" 1997. https://web.archive.org/web/20201204185440/http://commdocs.house.gov/committees/judiciary/hju41233.000/hju41233_0f.htm.

Vasvari, Raymond, and Gino Scarselli. "Law Professor Sues Federal Government Over Computer Privacy Issues" 1996. https://web.archive.org/web/20160930065605/https://www.eff.org/press/archives/2008/04/21-22.

Vasvari, Raymond, and Gino Scarselli. "Plaintiff Seeks Summary Judgment in Cleveland Case Challenging Licensing of 'Exports' of Cryptographic Information" 1996. https://web.archive.org/web/20060912162151/http://samsara.cwru.edu/comp_law/jvc/pressrel2.html.

Zimmermann, Phillip. “Testimony of Philip R. Zimmermann to the Subcommittee on Science, Technology, and Space of the US Senate Committee on Commerce, Science, and Transportation” 1996. https://web.archive.org/web/20201119111820/https://philzimmermann.com/EN/testimony/index.html.

Notes

[i] For a non-technical cryptology overview see Martin, *Cryptography*.

[ii] For a crypto wars history see Jarvis, *Crypto Wars*.

[iii] Advanced Telephony Unit, Federal Bureau of Investigation, "Impact of Emerging Telecommunications", 24.

[iv] Kapor, *Craig Jarvis Interview*.

[v] Barlow, "Jackboots on the Infobahn".

[vi] Clinton, "Address by President Bill Clinton".

[vii] Ibid.

[viii] Advanced Telephony Unit, Federal Bureau of Investigation, "Impact of Emerging Telecommunications", 24.

[ix] Ibid., 22.

[x] Ibid.

[xi] Zimmermann, "Testimony of Philip R. Zimmermann".

[xii] Ibid.

[xiii] For instance, see Abelson et al., "The Risks of Key Recovery".

[xiv] For instance, see Banisar, "Stopping Science".

[xv] For instance, see Butler and Forcht, "The Clipper Chip".

[xvi] For instance, see Froomkin, "The Metaphor Is the Key".

[xvii] For instance, see Pednekar-Magal and Shields, "The State and Telecom Surveillance".

[xviii] Ibid.

[xix] Pednekar-Magal and Shields, "The State and Telecom Surveillance".

[xx] Ibid., 461.

[xxi] Ibid.

[xxii] Ibid.

[xxiii] Esposti and Santiago-Gomez, "Acceptable Surveillance - Orientated Security Technologies", 437.

[xxiv] Ibid.

[xxv] Hughes, "US Domestic Surveillance after 9/11".

[xxvi] Strasheim, "Re: Zimmermann case".

[xxvii] Ibid., 143.

[xxviii] Esposti and Santiago-Gomez, "Acceptable Surveillance - Orientated Security Technologies".

[xxix] Greenwald, "NSA collecting phone records".

[xxx] Jarvis, "What caused the Clinton administration", 205-206.

[xxxi] Bryman, *Social Research Methods,* 467.

[xxxii] McCurley, "History of the IACR".

[xxxiii] Gonzalez-Barahona, "A Brief History".

[xxxiv] United States Congress, "S.266".

[xxxv] Advanced Telephony Unit, Federal Bureau of Investigation, "Impact of Emerging Telecommunications", 24.

[xxxvi] Markoff, "Data-Secrecy Export Case Dropped".

[xxxvii] United States Attorney, "US DoJ Zimmermann Press Release".

[xxxviii] Bernstein, "Curriculum Vitae".

[xxxix] Bernstein, "Declaration of Daniel J. Bernstein".

[xl] Ibid.

[xli] Electronic Frontier Foundation, "EFF Sues".

[xlii] Cohn, "Daniel J. Bernstein Vs United States".

[xliii] United States District Court Northern District of California, "Opinion", 1996.

[xliv] Ibid.

[xlv] The White House, "Executive Order 13026".

[xlvi] United States Department of Commerce, “EAR: Enforcement and Protective Measures”.

[xlvii] Ibid.

[xlviii] United States District Court Northern District of California, “Opinion”, 1997.

[xlix] United States Department of Justice, “Daniel J. Bernstein Vs United Department of State et al”; United States Court of Appeals for the Ninth Circuit, “Order”.

[l] Schneier, *Applied Cryptography Protocols*.

[li] Steinert-Threlkeld, “Cryptography tests rights”, 5F.

[lii] United States Department of State, “Request for Commodity Jurisdiction”.

[liii] Richey, “Memorandum Opinion”.

[liv] Clinton, “Statement on Signing the Telecommunications Act of 1996”.

[lv] Bass et al., “Stipulation and Proposed Scheduling”.

[lvi] United States Department of Commerce, “Letter from Patricia Sefcik”.

[lvii] Junger, “Declaration of Peter Junger”.

[lviii] Vasvari and Scarselli, “Law Professor Sues”; Vasvari and Scarselli, “Plaintiff Seeks Summary Judgment”.

[lix] United States District Court Northern District of Ohio Eastern Division, “Preliminary Injunction”.

[lx] The White House, “Executive Order 13026”.

[lxi] Scarselli, “Correspondence to the Department of Commerce”.

[lxii] United States Congress, “S.974”.

[lxiii] Ibid, Section 1030.

[lxiv] Burns, “Open Letter”.

[lxv] National Research Council, “Cryptography's Role”.

[lxvi] Ibid., 13.

[lxvii] Ibid., 6.

[lxviii] Ibid.

[lxix] Ibid., 7.

[lxx] Ibid., 8.

[lxxi] President's Export Council Subcommittee on Encryption, "Findings".

[lxxii] Ibid., 122.

[lxxiii] Ibid.

[lxxiv] For instance, see statement of the Computer and Business Equipment Manufacturers Association quoted in Pednekar-Magal and Shields, "The State and Telecom Surveillance", 444.

[lxxv] Baker, *Craig Jarvis Interview*.

[lxxvi] Ibid.

[lxxvii] Ibid.

[lxxviii] Ibid.

[lxxix] Ibid.

[lxxx] Ibid.

[lxxxi] Mulivor, "SPA Press Release".

[lxxxii] Ibid.

[lxxxiii] Abelson, et al., "The Risks of Key Recovery".

[lxxxiv] The White House, "Administration Statement".

[lxxxv] Ibid.

[lxxxvi] Ibid.

[lxxxvii] Ibid.

[lxxxviii] Apple, Atalla et al., "Joint Press Announcement".

[lxxxix] Ibid.

[xc] Ibid.

[xci] United States House of Representatives, "Hearing on H.R. 695", 41.

[xcii] Lash, “Computer Alliance Supports Encryption”.

[xciii] Markoff, “U.S. Rebuffed in Global Proposal”; OECD, “Recommendation of the Council”.

[xciv] Aldrich, *GCHQ*, 476.

[xcv] Markoff, “U.S. Rebuffed in Global Proposal”; OECD, “Recommendation of the Council”.

[xcvi] Andrews, “Europeans Reject U.S. Plan”.

[xcvii] Schneier, *Craig Jarvis Interview*.

[xcviii] Ibid; Denning, *Craig Jarvis Interview*; Kapor, *Craig Jarvis Interview*.

[xcix] George, *Craig Jarvis Interview*.

[c] Kapor, *Craig Jarvis Interview*.

[ci] McConnell, *Craig Jarvis Interview*.

[cii] Baker, *Craig Jarvis Interview*.

[ciii] Bidzos, *Craig Jarvis Interview*.

[civ] Denning, *Craig Jarvis Interview*.

[cv] Ibid.

[cvi] Miller, *Craig Jarvis Interview*.

[cvii] Ibid.

[cviii] Ibid.

[cix] Kapor, *Craig Jarvis Interview*.

[cx] McConnell, *Craig Jarvis Interview*.

[cxi] Denning, *Craig Jarvis Interview*.

[cxii] Schneier, *Craig Jarvis Interview*.

[cxiii] George *Craig Jarvis Interview*.

[cxiv] Ibid.

[cxv] Baker, *Craig Jarvis Interview*.

[cxvi] Ibid.

[cxvii] Dempsey, *Craig Jarvis Interview*.

[cxviii] McConnell, *Craig Jarvis Interview*.

[cxix] Baker, *Craig Jarvis Interview*.

[cxx] Dempsey, *Craig Jarvis Interview*.

[cxxi] Baker, *Craig Jarvis Interview*.

[cxxii] Ibid.

[cxxiii] Bidzos, *Craig Jarvis Interview*.

[cxxiv] National Research Council, "Cryptography's Role in Securing the Information Society", 1.

[cxxv] Dempsey, *Craig Jarvis Interview*.; Rotenberg, *Craig Jarvis Interview*.

[cxxvi] Markoff, "U.S. Rebuffed in Global Proposal".

[cxxvii] Dempsey, *Craig Jarvis Interview*.; Rotenberg, *Craig Jarvis Interview*.

[cxxviii] Ibid.

[cxxix] Rotenberg, *Craig Jarvis Interview*.

[cxxx] McConnell, *Craig Jarvis Interview*.

[cxxxi] Bidzos, "Nothing Safe About Encryption Bills".

[cxxxii] Bidzos, *Craig Jarvis Interview*.

[cxxxiii] McConnell, *Craig Jarvis Interview*.

[cxxxiv] Denning, *Craig Jarvis Interview*.

[cxxxv] Ibid.

[cxxxvi] Reinsch, *Craig Jarvis Interview*.

[cxxxvii] George *Craig Jarvis Interview*.

[cxxxviii] Blaze, "Protocol Failure".

[cxxxix] Brantly, "Banning Encryption to Stop Terrorists", 29; Riebe, et al., "U.S. Security Policy", 59-60.

[cxl] Blaze, "Key Escrow from a Safe Distance", 2.1.

[cxli] Rotenberg, *Craig Jarvis Interview*.

[cxlii] Dempsey, *Craig Jarvis Interview*.

[cxliii] Levy and Robinson, "Principles for a More Informed Exceptional Access Debate".

[cxliv] For instance, see Levy and Robinson, "Thoughts on Child Safety".

[cxlv] For instance, see Portnoy, "Why Adding Client-Side Scanning Breaks End-To-End Encryption"; Open Rights Group, "Online Safety Bill".

[cxlvi] Greenwald and MacAskill, "NSA Prism program".

[cxlvii] Ibid.

[cxlviii] Ibid.

[cxlix] Ibid.

[cl] Ibid.

[cli] Ibid.

[clii] Ibid.

[cliii] Ibid.

[clvii] Jarvis, *Crypto Wars*, 351-361.

[clviii] Rozenshtein, "Surveillance Intermediaries", 99.

[clix] Ibid., 186-187.

[clx] Ibid., 188-189.

[clxi] Dempsey, *Craig Jarvis Interview*.

[clxii] Baker, *Craig Jarvis Interview*.

[clxiii] Ibid.

[clxiv] Rotenberg, *Craig Jarvis Interview*.