Timeline of Intelligence Surveillance Scandals

Shen Ibrahimsadeh, Ibtehal Hussain, Bernardino Leon Reyes, Ronja Kniep, Félix Tréguer, Emma Mc Cluskey, Claudia Aradau

Timeline of Intelligence Surveillance Scandals

December 2022

This research report compiled for the GUARDINT research project[1] collates short case-studies of scandals around intelligence surveillance in France, Germany, the United Kingdom and the United States. It is co-authored by Shen Ibrahimsadeh (WZB), Ibtehal Hussain (King's College London), Bernardino Léon Reyes (CERI Sciences Po), Ronja Kniep (WZB), Félix Tréguer (CERI Sciences Po), Emma Mc Cluskey (University of Westminster), Claudia Aradau (King's College London). Summaries of case studies can be explored as an online timeline with TimeLineJS.

Table of Contents

1. GUARDINT is a European research project that examines surveillance, intelligence and oversight. The main goal is to build empirical and conceptual tools to better understand the limits and potential of intelligence oversight mechanisms. Teams from leading research institutions in France, Germany and the United Kingdom are contributing to the 3-year collaborative project (2019-2022). Cross-disciplinary in nature, our work encompasses policy and legal analysis as well as sociological and historical research.

DE 1957-03-23: The Dubois Affair

In 1957, the Swiss federal public prosecutor René Dubois killed himself, allegedly as a consequence of having been involved in illegal intelligence sharing with the French foreign intelligence agency SDECE. At the time, media reported that he had shared documents – telephone intercepts of the Egyptian embassy in Bern talking to Cairo – with Marcel Mercier who worked for the French SDECE. Back then, oversight was deliberately undermined by a joint strategy of German and French intelligence agencies that included threats to Swiss authorities with compromising material. Instead of leading to reform or more oversight, the scandal and its handling by connected agencies lead to an obfuscation and strengthening of transnational intelligence ties.

Starting point*:* The 'smoking gun' of this intelligence scandal was an officer's pistol. It was fired on 23 March 1957 by the Swiss federal public prosecutor René Dubois who shot himself in his apartment in Bern. Three days before, international media, among them the US-American news agency *Associated Press* and the *Tribune de Genève*, reported about investigations against a Swiss police officer – Max Ulrich – who was accused of illegal information sharing with the French. Internal investigations started to evolve when in October 1956, the head of the press agency *Universum Press* in Geneva informed the Swiss Department of Justice and Police that he was in possession of information according to which federal prosecutor Dubois exchanged confidential material with the French 'attaché' Marcel Mercier – later described in the press as a "seasoned routineer in international intelligence". As Dubois' death followed public reports on the information sharing, it seemed that he killed himself under the pressure of the revelations. Back then, his suicide was perceived as a plea of guilty.

Wider intelligence-related context: The public scandal evolved around the illegal information sharing that questioned Switzerland's presumed neutrality in the Algerian War. The shared telephone intercepts of the Egyptian embassy contained information on Egypt's support for the Algerian resistance; and the content of related intelligence reports had been leaked to the press. Yet, the events leading to the "Dubois affair" have to be understood as a product of the internal struggles and transnational allegiances of security agencies in postwar Europe. In the middle of the 1950s, Dubois – a social democrat who has been characterised as "anti-German" and "anti-military" (Krieger, 2021, p. 288) – started investigations into Swiss money laundering and intelligence gathering for National Socialists (Tarli, 2019). This was met with internal resistance by the Swiss police, including Max Ulrich, who obstructed Dubois' investigation through gathering compromising information on Dubois through his connection to French intelligence. In fact, both Dubois and Ulrich had been engaging in close exchanges with the French intelligence agencies through Marcel Mercier and had asked him for help in their different causes. Yet, when Dubois, shortly before his death, agreed to arrest Max Ulrich, Mercier intervened. He visited the Swiss police to tell them that Max Ulrich was innocent, and that he had received the sensitive material from Dubois through official channels, not through Ulrich, adding: "Les Français ont assez de preuves pour faire sauter le Procureur général" – "The French have enough evidence to blow up the federal public prosecutor" (Bundesrat, 1958, p. 679).

Transnational dimension: The intention of Merciers' intervention was not only to protect Ulrich but another intelligence connection: the ties to the recently founded, German foreign intelligence agency BND, that Ulrich was also in close exchange with. As part of the connection, the SDECE had asked both the German and Swiss agencies for intelligence sharing related to Egypt and Syria who supported Algerians (Krieger, 2021, p. 287). As is known today from historic archives, the intelligence report about Egypt's arms supplies to Algerian rebels had not only been shared with the BND but also with '"the British"' (ibid., p. 289) before it had been leaked to the press. The Swiss investigations and the death of Dubois had presented a threat to the quite recent but already close ties the BND had established to its French counterparts through the 'intelligence tandem' of Marcel Mercier and Harald Mors, partly on Swiss territory and with involvement of Swiss security agencies. Therefore, as archival material shows, the two agencies agreed on a joint handling of the Dubois affair during a visit in Paris in December 1957 (Krieger, 2021, p. 289). An internal report by Harald Mors (BND) openly declares: "The SDECE's strategy was to threaten the Swiss authorities with compromising revelations 'that would thwart a whole row of leading Swiss personnel." (ibid.). A historian recently résumés: "Fortunately for the 'Pullach-Paris axis' (…) both sides used the affair to tighten the bonds

between their foreign services. Mercier was ordered to Munich and installed as SDECE resident in the French Consulate General there".

Change in oversight: The Dubois Affair triggered an investigation by the Swiss Bundesrat (1958). The report concluded that both Max Ulrich and Dubois had been involved in illegal information sharing. Max Ulrich had been sentenced to roughly two years of prison for violation of official secrets and political espionage due to his comprehensive sharing of confidential reports with Mercier. Despite revealing some important details, in retrospect, the report is described as incomplete (Tarli, 2019), in particular its conclusion that "the scope of the affair remained limited to Federal Prosecutor Dubois and Inspector Max Ulrich" (Bundesrat, 1958, p. 680). It framed the sharing of secrets and mixing private and public matters as personal failures of otherwise respectable officials. Criticism of the institutional settings that arose after the affair was responded to by justifying the status quo. (ibid. p. 691f).

References

Bundesrat (1958). *Bericht des Bundesrates an die Bundesversammlung über die Vorkommnisse, die mit dem Hinschied von Bundesanwalt Dubois in Zusammenhang standen und zur Verurteilung des Bundespolizei-Inspektors Max Ulrich führten.* (No. 7622). Available at: https://www.amtsdruckschriften.bar.admin.ch/viewOrigDoc.do?ID=10040310

Krieger, W. (2021). *Partnerdienste. Die Beziehungen des BND zu den westlichen Geheimdiensten 1946-1968: Veröffentlichungen der Unabhängigen Historikerkommission zur Erforschung der Geschichte des Bundesnachrichtendienstes 1945–1968*. Berlin: Christoph Links Verlag.

Media archives

A Prato, C. (1957, March 26). Vive émotion en Suisse après le suicide du procureur fédéral Dubois. *Le Monde*. https://www.lemonde.fr/archives/article/1957/03/26/vive-emotion-en-suisse-apres-le-suicide-du-procureur-federal-dubois_2334154_1819218.html

A Prato, C. (1957, March 27). Deux journaux de Suisse alémanique mettent en cause l'attaché commercial de l'ambassade de France. *Le Monde*. https://www.lemonde.fr/archives/article/1957/03/27/deux-journaux-de-suisse-alemanique-mettent-en-cause-l-attache-commercial-de-l-ambassade-de-france_2332933_1819218.html

Am Telephon unvorsichtig. (1957, April 2). *Der Spiegel*. https://www.spiegel.de/politik/am-telephon-unvorsichtig-a-247c0264-0002-0001-0000-000041120849

L'inspecteur Ulrich a avoué avoir transmis des documents au colonel Mercier. (1957, May 18). *Le Monde.* https://www.lemonde.fr/archives/article/1957/05/18/l-inspecteur-ulrich-a-avoue-avoir-transmis-des-documents-au-colonel-mercier_2334863_1819218.html

Tarli, R. (2019, January 16). Die verlorene Ehre des René Dubois. *Blick*. https://www.blick.ch/life/wissen/geschichte/verschwoerung-gegen-bundesanwalt-die-verlorene-ehre-des-rene-dubois-id15109526.html

US 1960-09-06: The Martin and Mitchell Affair

In the summer of 1960, two cryptographers from the National Security Agency defected to the USSR and held a press conference in Moscow. Presenting themselves as pacifists, William Martin and Bernon Mitchell disclosed the global surveillance practices at the NSA, which they claimed endangered world security. Quickly chastised as "sexual deviates" by officials in Washington, the two men shed light on the secretive world of signal intelligence and arguably played a role in the politicisation of new a generation of civilian cryptographers keen on protecting people's communications from state surveillance.

Starting point: In the summer of 1960, two NSA cryptographers, William Martin and Bernon Mitchell left their jobs to go on vacation together, eventually defecting to Russia seeking political asylum. On 6 September, the pair held a press conference in Moscow. At that time, the work conducted at the NSA was still mostly secret,

and in their interventions the two whistleblowers aimed to shed some light on its practices. The United States, they explain in their statement, "intercepts and decrypts (. . .) the secure communications of more than forty nations, including those of its own allies."

Wider intelligence-related context: Since the early days of the Cold War, the NSA and its UK partner, GCHQ, had reigned supreme over the surveillance of international communications, investing huge sums in building intercept stations and mastering encryption and cryptanalysis. One of their priorities was obviously to prevent any transfer of knowledge in this field to the Soviet bloc. The defection of the two officers immediately appeared as a historic setback.

Transnational dimension: More than half a century before the Snowden affair, Martin and Mitchell's press conference revealed the existence of a vast network of 2000 interception stations scattered around the world and in which more than 8000 operators and analysts worked every day. For these SIGINT operations, the US government spent the annual sum of half a billion dollars. The two men went on to reveal the existence of the NSA headquarters at Fort Meade, whose basements they said were filled with computers. The US, they went on to explain, also sold rigged cryptographic machines to allied countries and nurtured a strong collaboration with the UK's GCHQ in the field of cryptanalysis (the two countries had sealed their alliance in the field of technical intelligence in 1946, with the signing of the UKUSA agreement). Taking the American public as witness, Martin and Mitchell considered that such activities – in particular the regular violation of the airspace of sovereign countries for espionage purposes – amounted to provocations which, in the context of the nuclear arms race, put world peace at risk (Barrett, 2009; Anderson, 2007).

Change in oversight: These staggering disclosures were immediately denounced by the American establishment. Congressman Francis E. Walter, chairman of the House Un-American Activities Committee (HUAC), spread the rumor that Martin and Mitchell were "sex deviates" because of their alleged homosexuality, while President Eisenhower called the two man "traitorous". Meanwhile, representatives of the Department of Defense denied their claims as being "falsehoods" spurred by "Russian propaganda" (Caruthers, 1960). The defection was such an embarrassment that a two-year congressional investigation was started. Eventually, the NSA overhauled its recruitment and security procedures to avoid new defections.

Martin and Mitchell were granted Soviet citizenship and neither of them would ever go back to live in the United States. Their defection, which had broken open one of America's best-kept secrets, piqued the curiosity of a journalist by the name of David Kahn, who had been working for several years on a book on the history of cryptography. In reaction to the scandal, Kahn decided to devote a whole chapter to the NSA. In turn, the agency placed Kahn under surveillance and tried to prevent the publication of the book, ultimately succeeding in having three contentious passages removed (Levy, 2001, p. 22-25). When it came out in 1967, Kahn's book, *The Codebreakers*, became the bedside book of a new generation of young mathematicians socialised in the then-rebellious atmosphere of American campuses. From the 1970s onwards, they would undermine the monopoly of the military and of intelligence on cryptography and exert forms of oversight by calling out NSA's plans to tamper with civilian cryptographic products (Corrigan-Gibbs, 2004).

References

Barrett, D. M. (2009). Secrecy, Security, and Sex: The NSA, Congress, and the Martin–Mitchell Defections. *International Journal of Intelligence and CounterIntelligence*, *22*(4), 699–729. https://doi.org/10.1080/08850600903143320

Levy, S. (2001). *Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age* (1st edition). Penguin Books.

Corrigan-Gibbs, H. (2014). Keeping Secrets. *Stanford Magazine*, *November/December*. https://alumni.stanford.edu/get/page/magazine/article/?article_id=74801

Media archives

Text of Statements Read in Moscow by Former U.S. Security Agency Workers. (1960, September 7). *The New York Times*, 10. https://timesmachine.nytimes.com/timesmachine/1960/09/07/99869277.html?pageNumber=10

Anderson, R. (2007, July 17). The Worst Internal Scandal in NSA History Was Blamed on Cold War Defectors Homosexuality. *Seattle Weekly*. https://www.seattleweekly.com/news/the-worst-internal-scandal-in-nsa-history-was-blamed-on-cold-war-defectors%C2%92-homosexuality/

Caruthers, O. (1960, September 7). Two Code Clerks Defect to Soviet: Score U.S. "Spying." *The New York Times*. https://www.nytimes.com/1960/09/07/archives/war-threat-seen-security-agency-men-decry-flights-over-alien.html

Defectors Expect More U.S. Spying: 2 Who Fled to Moscow From Security Agency Appraise Kennedy. (1960, December 20). *The New York Times*. https://www.nytimes.com/1960/12/20/archives/defectors-expect-more-us-spying-2-who-fled-to-moscow-from-security.html

DE 1963-08-27: The Pätsch Affair

In 1963, Werner Pätsch, a clerk at the German domestic intelligence agency, the Bundesamt für Verfassungsschutz (BfV) (the Federal Office for the Protection of the Constitution), became the first whistleblower to leak the secrets of modern German intelligence to the press. He documented the illegal, unauthorised tapping of postal and telephone communications of German citizens by the BfV with the help of an undisclosed "allied security agency", as well as the employment of former SS officers from the Third Reich security apparatus by the BfV. Pätsch was prosecuted for betrayal of secrets. In the end, the court ruled in his favour. The affair contributed to the establishment of the G10 Commission, one of the main oversight bodies in modern Germany.

Starting point: On August 27th 1963, the magazine *Stern* published a cover story titled "Der Mann ohne Namen" ("The Man without a Name"), which suggested that some Nazis were employed by the German Bundesamt für Verfassungsschutz (BfV). One week later, in early September, the newspaper *Die Zeit* published an article that attracted huge public attention (Foschepoth, 2014, 120; Die Zeit, 1963). The article raised doubts about statements of the then Minister of Interior Hermann Höcherl on the numbers of Nazis employed by the BfV. *Die Zeit* published a list of names, thus challenging Höcherl's claim that no more than 2% of the staff (16 persons) within the BfV had such a background (Die Zeit, 1963). The article quoted a source familiar with the matter, which would later turn out to be Werner Pätsch.

Pätsch's job at the BfV consisted in analysing intercepted letters of German citizens. He decided to leak classified information to the lawyer Joseph Augstein, brother of *Der Spiegel* publisher Rudolf Augtein. However, it was not *Spiegel*, but *Zeit* that initially raised public scrutiny with their reporting that relied on Pätsch's whistleblowing (Die Zeit 2013). Thus, Pätsch's whistleblowing revealed that there were significant numbers of former Nazis working for the BfV. As the article stated:

Höcherl's ministry officials trivialise the extent of the activities of former members of such Nazi organisations, which are now particularly badly remembered. Only "a few" constitutional protectors, they say, came from the SS, the SD or the Gestapo, they had – which in many cases is not at all true – only possessed "SS affiliation grades" and belonged only to a "nominal SD formation" which at the time had been excluded by the Nuremberg prosecuting authority. (Die Zeit, 1963).

Wider intelligence-related context: The article revealed how the BfV systematically circumvented the German constitution (especially its Article 10 on postal communication) by tapping into the phone calls and opening letters of hundreds of German citizens without any legal basis. Up to 15,000 of such orders were conducted between 1961-1963 according to the BfV (Foschepoth, 2014, 125). There was also some suspicion that members of the government had been subjected to these practices (Die Zeit, 1963). The government denied these practices but pressure for reform and evidence increased. Meanwhile, Pätsch seeked to protect himself from being "taken out" by the BfV. He thus chose to revealed his identity in the *Spiegel* and gave an interview; on his motives he said:

> "I have been involved in the surveillance of people's mail and telephones for years, and certain recent incidents have caused me to have more and more conflicts of conscience about whether my activities are in accordance with the constitution." (Spiegel, 1963)

Transnational dimension: Pätsch's main contribution, however, was probably the disclosure of the BfV's relationship to a not specified foreign entity, likely an intelligence agency of the allied forces. The joint surveillance was said to be conducted on the basis of a legal provision for telecommunication interception by the allied forces at that time – Article 4 and 5 of the 1955 Treaty on Germany granted them the right to tap telephone conversations and censor letters (Die Zeit, 1963). However, this was an abusive interpretation of the article, as the latter only allowed allied forces to conduct these measures and at no point foresaw a sharing of information with German security institutions (Sommer, 1963). The BfV could exploit the surveillance privilege of the allied forces also because the allies did not demand any explanation from the BfV, when asked to conduct surveillance. To justify the resort to the allied privilege of surveillance the BfV claimed that the security of allied forces was at risk (Zeit, 2013).

Change in oversight: German Chancellor Konrad Adenauer, who was in his final days in office, claimed that there were no shortcomings by the leadership of the BfV and that further deterioration of the BfV's image was not in the interest of the government. Furthermore, he shared his impression: "(…) that many critics are less concerned with upholding the constitution than with blaming the federal government and undermining the state's reputation." (Foschepoth, 2014, 122). He pointed out the communist threat in Germany, implicitly justifying the surveillance and downplaying the scandal. The two largest political parties were reserved, although a demand was made within the Interior Committee of the Bundestag for the Ministry of Interior to cease such activities. The Ministry denied that request and ordered a memo to the allied agencies that reaffirmed the commitment to use such surveillance techniques. Furthermore, the first parliamentary oversight body, the Parlamentarischen Vertrauensmännergremiums (PVMG) which was tasked to oversee activities of the Bundesnachrichtendienst (BND), had additionally been tasked to include the BfV in their sphere of responsibility, due to Pätsch's revelations. However, the PVMG had no real tools to enforce any sanctions against the government or the agencies (Gehring, 2019).

An inquiry committee was established and its final report concluded that "abuses have not been detected". The report also demanded that the Federal Government present "proposals on parliamentary control of the intelligence services" by 1 October 1964 (Final Report of the Bundestag Inquiry, 1963). Among other things, these proposals later led to the limitation of Article 10 of the German Constitution (Grundgesetz) alongside the bigger amendment of the German Emergency Acts in 1968. In order "to protect the free democratic basic order of the Federation and the States", the tapping of communication of German citizens could be legal only in certain cases, such as terrorism or violent acts against the state. To oversee wiretapping by intelligence agencies, a new G10 Commission was established with the task of upholding Article 10 of the German Constitution, which guarantees the secrecy of correspondence, post and telecommunications. (Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses, 1968). At intervals of no more than six months, the Federal Minister of the Interior had to inform the Commission about interception measures. The Commission was able to declare measures as inadmissible or not necessary. In such cases, the competent Federal Minister had to give up on these measures without delay (Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses, 1968, § 9.2). This Commission is still active and is considered one of the main intelligence oversight institutions in Germany.

References

Bundesgesetzblatt, Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (1968). https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl168s0949.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl168s0949.pdf%27%5D__1653060387166

Final report of the second Inquiry Committee of the German Bundestag, printed matter IV/1544 (1963). https://dipbt.bundestag.de/doc/btd/04/021/0402170.pdf

Nehring, C. (2019, May 24). *Nachrichtendienste in Deutschland. Teil 1*. Bundeszentrale für politische Bildung. https://www.bpb.de/geschichte/zeitgeschichte/deutschlandarchiv/292006/nachrichtendienste-in-deutschland-teil-i

Foschepoth, J. (2013). *Überwachtes Deutschland: Post- und Telefonüberwachung in der alten Bundesrepublik*. Göttingen: Vandenhoeck & Ruprecht.

Media archives

Absolut sichere Quelle (1963, October 01). *Der Spiegel.* https://www.spiegel.de/politik/absolut-sichere-quelle-a-4a06fa89-0002-0001-0000-000046172126

Johst, D. (2013, November 07). Der Edward Snowden der Sechziger. *Die Zeit*. https://www.zeit.de/2013/46/abhoer-affaere-werner-paetsch-1963/komplettansicht#

Sagte Höcherl die Wahrheit? (1963, September 6). *Die Zeit*. https://www.zeit.de/1963/36/sagte-hoecherl-die-wahrheit/komplettansicht

Slähle, P. (1963, October 11). Zwischenbilanz in der Abhör-Affäre. *Die Zeit*. https://www.zeit.de/1963/41/zwischenbilanz-in-der-abhoer-affaere/komplettansicht

Sommer, Theo (1963, September 13). Nur Abhör-Amtshilfe? *Die Zeit.* https://www.zeit.de/1963/37/nur-abhoer-amtshilfe/komplettansicht

US 1070-1-17: The CONUS Intel Scandal

In January 1970, former Army captain Christopher Pyle revealed that the US Army had engaged in a vast and illegal effort aimed at building databases on domestic dissidents. The ensuing scandal, known as the CONUS Intel scandal, led to the first full-fledged Congress investigation in intelligence surveillance. Despite its limited legacy on the regulatory level, it still propelled abuse of intelligence agencies to the forefront of public debate.

Starting point: In January 1970, as the war in Vietnam and the debate on American imperialism tore the U.S. apart, the Washington Monthly published a 13-page report by Christopher Pyle, a PhD student at the Law School of Columbia University. Born in 1939, Pyle had been a reserve officer after graduating from law school and a young law professor at the Army Intelligence School in Baltimore from 1966 to 1968. Just out of military service, he needed to let the American public know about what he had witnessed, turning into both a reporter and whistleblower. First declined by the New York Times,he reached out to the Washington Monthly to publish his report (Pyle, 2022). In his article, Pyle disclosed that through a program entitled CONUS Intel (where CONUS stands for "Continental US"), the army had "1,000 plainclothes investigators, working out of some 300 offices from coast to coast, [to] keep track of political protests of all kinds, from the [Ku Klux] Klan rallies to anti-war speeches at Harvard" (Pyle, 1970a). For the first time, the details of this vast domestic surveillance enterprise that had started in 1965 were made public.

At the beginning, Pyle explained in his article, the Army only sought to monitor "early warnings" of potential civil disorders which legally could justify domestic military intervention if the civilian authorities called for the Army's help to restore peace and order. With the uprisings of Black ghettos in the summer of 1967, the Army's surveillance capabilities expanded massively. CONUS then saw "its scope widened to include the political beliefs and actions of individuals and organisations active in the civil rights, white supremacy, black power, and anti-war movements" (Pyle, 1970a). Data was collected through monitoring subscriptions to radical magazines, undercover agents, paid informants, and voluntary civilians. Whilst Pyle's article was being published and syndicated in more than 41 news outlets across the U.S., CONUS Intel was going digital, as the Army was in the process of linking "its teletype reporting system to a computerised data bank (…) installed at the Investigative Records Repository at Fort Holabird in Baltimore".

Wider intelligence-related context: By 1970, the U.S. national security establishment was undergoing an unprecedented backlash. After an early phase of the Cold War marked by political orthodoxy and anti-leftism, the late 1960 saw the political consensus around intelligence and domestic surveillance shatter into pieces (Keller, 1989). The grip and influence of the national security establishment on the economy, university, popular culture, and the political field was undermined, as an array of new radical social movements swept the country and questioned U.S. reliance on segregation at home and imperialism abroad. Meanwhile, with rampant computerisation, there were increasing fears of a "Big Brother" state. From the early sixties

onwards, people acrossU.S. society – including student protesters, computer engineers, and congress members – began objecting to the growing use of computers by the U.S. government (Lepore 2020).

In the midst of all this opposition, intelligence agencies reacted by backsliding in their old habits, expanding the surveillance of social movements (Prados & Nichter, 2020), whilst making use of the new information processing machines of the day to support that expansion. As the Federal government enlisted many research teams to turn these technologies into predictive devices, more mundane innovations made their ways into intelligence and law enforcement practices. For instance the FBI's National Crime Information Center was launched in 1967 to give "all local officers, whether they have their own departmental computers or not" access to federal crime databases (Hoover, 1967) . But, as it would turn out, this was just one publicised example of a myriad of such developments all across the world of police and intelligence.

Change in oversight: Pyle's disclosures of the the CONUS Intel program would lead to the first full-fledged congress inquiry into intelligence affairs, two years before the Watergate scandal and five years before the Church committee (see below). "Back then, nobody had ever taken on the intelligence community, so there was some fear of the unknown", Pyle recalls in an interview (Pyle 2022). He was eventually convinced to join the committee investigation of Democratic Senator Sam Ervin from North Carolina, whom Pyle then knew for his legalistic defence racial segregation (which, as Pyle commented years later, was "'not an auspicious beginning"). But he was convinced that Ervin could advance civil rights, and understood that his conservative credentials and former experience as an army officer would serve as protection. Still, from fear of generating backlash against his initiative from J. Edgar Hoover or other powerful heads of intelligence agencies, the so-called "Ervin Committee" left out any reference to intelligence in its title, instead choosing to call its hearings "Federal Data Banks, Computers, and the Bill of Rights."

Within a month of Pyle's first article on CONUS Intel, SAHMthe Ervin Committee was holding hearings, with testimonies by prominent representatives of the computer industry, the ACLU, civil servants working on computerised law enforcement databases, and most crucially, former military intelligence agents. Meanwhile, Pyle prepared the bulk of the committee report entitled "Army Surveillance of Civilians", having recruited more than 120 former intelligence agents to supply information about the program (the report would only be published in 1973). In June of 1970, Pyle had published another article uncovering how the Army had sought to cover-up the program and reinstated it (Pyle, 1970b). In late 1970, the sitting Secretary of Defense – who had apparently been left in the dark by the Military about the extent of the CONUS program – had to pledge to rein in the Army's domestic surveillance activities (Franklin 1970). Despite orders issued by congress to destroy the illegal files the Army had collected, investigators could not ascertain that destruction orders had been respected. As it would turn out, they were not. In June 1975, NBC journalist Ford Rowan disclosed that computerised CONUS files had actually been transmitted to the NSA via a new computer network known as the ARPANet – the ancestor of the Internet – with the help of computer scientists from MIT and Harvard. The goal was apparently to provide real-world data to feed into the research of predictive models (Levine, 2018).

In the Spring of 1971, as Pyle and other staff worked on the Ervin committee reports, it was revealed that the Army's domestic surveillance program included members of congress. The Democratic Party then reacted by establishing a Planning Group on Intelligence and Security which worked in the subsequent months on a plan to reform the intelligence community and later came up with a radical list of demands (e.g. the automatic declassification of government documents after 3 years; the protection of reporters when disclosing sources; the banning of government agents from masquerading as journalists, etc.) (Blum, 1972). Beyond the Pentagon, the whole Intelligence Community was starting to feel the heat.

The Ervin committee's hearings and report (which was eventually published in 1973 after Ervin fought the Department of Defense to authorise its declassification) brought to light dozens of ongoing computerised intelligence gathering operations across federal and local government agencies. It also further inscribed the issue of privacy on the legislative agenda, with Senator Ervin pushing for new data protection regulations (Franklin, 1970). This process culminated with the adoption of the Privacy Act in 1974. In 1973, Ervin had also tabled the "Freedom From Surveillance Bill", which sought to make domestic surveillance by the Army a criminal offence (Ervin 1973), but it was never adopted.

Meanwhile, the ACLU started a legal challenge by Arlo Tatum, the executive secretary of the Central Committee for Conscientious Objectors, against the Secretary of Defense for the surveillance Tatum was subject to due to CONUS Intel. 29 of Pyle's army informants filed a brief in support of the claimant. However, the motion was dismissed by the Supreme Court in 1972 on the grounds that the claimant could not prove he had suffered any harm or injury as a consequence of government spying. The ruling, *Laird v. Tatum*, has never been overturned, meaning that to this day the fear of potential harm – or a "chilling effect" – of a surveillance program is not enough to challenge it.

Despite limited regulatory legacy, Pyle's revelations and the findings of the Ervin committee on federal "data banks" created a precedent. Seen in this light, and paying attention to the many controversies around the overreach of government surveillance that took place from 1970 to 1975, these attempts should be read as a starting point in the history of U.S. intelligence oversight.

References

Army Surveillance of Civilians: A Documentary Analysis (Report of the Subcommittee on Constitutional Rights, Comm. on the Judiciary). (1972). US Senate.

Military Surveillance of Civilian Politics (Report of the Subcommittee on Constitutional Rights, Committee on the Judiciary). (1973). U.S. Senate. https://ia601906.us.archive.org/18/items/Military-Surveillance-Civilian-Politics-1973/MilitarySurveillanceCivilianPolitics.pdfh

Blum, R. H. (1972). *Surveillance and Espionage in a Free Society* (Report by the Planning Group on Intelligence and Security of the Polity Council). Democratic National Party.

Ervin, S. (1973). Freedom From Surveillance Bill. https://www.congress.gov/bill/93rd-congress/senate-bill/2318

Federal Data Banks, Computers, and the Bill of Rights (Hearings before the Subcommittee on Constitutional Rights of the Committee on the Judiciary). (1971). U.S. Senate.

Keller, W. (1989). The Liberals and J. Edgar Hoover : Rise and Fall of a Domestic Intelligence State. Princeton University Press.

Lepore, J. (2020). If Then : How the Simulmatics Corporation Invented the Future. Liveright.

Levine, Y. (2018). Surveillance Valleys: The Secret Military History of the Internet. PublicAffairs.

Military Surveillance of Civilian Politics (Report of the Subcommittee on Constitutional Rights, Committee on the Judiciary). (1973). U.S. Senate. https://ia601906.us.archive.org/18/items/Military-Surveillance-Civilian-Politics-1973/MilitarySurveillanceCivilianPolitics.pdf

Prados, J., & Nichter, L. A. (2020). Spying on Americans : Infamous 1970s White House Plan for Protest Surveillance Released. National Security Archive Briefing Book, 712. https://nsarchive.gwu.edu/briefing-book/intelligence/2020-06-25/spying-americans-new-release-infamous-huston-plan

Pyle, C. (2022, May 20). Looking back at the CONUS Intel Scandal (F. Tréguer) [Telephone interview].

Westin, A. (1967). *Privacy and Freedom*. New York:Anthenum.

Media archives

Franklin, B. A. (1970, December 27). Surveillance of Citizens Stirs Debate. The New York Times. https://www.nytimes.com/1970/12/27/archives/surveillance-of-citizens-stirs-debate-government-surveillance-of.html

Hoover, J. E. (1967, January). Now: Instant Crime Control in Your Town. Popular Science, 67.

Pyle, C. H. (1970, January). CONUS Intel: The Army Watches Civilian Politics. The Washington Monthly, 2(1), 4-16.

Pyle, C. H. (1970, July). CONUS Revisited: The Army Covers Up. The Washington Monthly, 2(5), 49-58.

FR 1974-03-21: The Safari Affair

In 1974, France's leading newspaper Le Monde *ran a story revealing that the Ministry of the Interior was working on a centralised system interconnecting all the databases held by some of the biggest public administrations (law enforcement agencies, the Ministries of Justice and Labour, the army, welfare services, etc.). In a context marked by strong criticism against the computerization of state bureaucracies and the illiberal impulses of intelligence agencies, these revelations led to a scandal and the institutionalisation of new oversight mechanisms a few years later, with the adoption of a data protection framework and of the French data protection authority, the CNIL.*

Starting point: On March 21st, 1974, the French daily *Le Monde* ran a story on the "SAFARI database," a system that had been in the works for several years but whose exact scope remained unknown. According to Boucher, rather than the mere digitization of civil registries, the ministry of the Interior was actually working on a centralised system interconnecting all the databases held by some of the biggest public administrations (law enforcement agencies, the Ministries of Justice and Labour, the army, welfare services, etc.) (Boucher, 1974). He explained that it was based on a powerful computer developed under a public research programme, the Iris-80. In his article, Le Monde's reporter, Philippe Boucher – who apparently got the story from a computer engineer turned whistleblower was stunned to discover that the whole project had been veiled in secrecy, and that the government had sought to bypass the Parliament. "We have every reason to doubt the purity of this endeavour," he wrote, "considering how much care is given to conceal its implementation."

Wider intelligence-related context: In the post-1968 zeitgeist, Boucher's article tapped into growing anxieties about computer surveillance. In France, police forces were starting to turn their files into digital formats (Heilmann 2005), while intelligence agencies poured vast resources into computers to store data and break cryptographic codes (Le Monde 1972). Le Monde's disclosures also came at a turbulent time: the minister of the Interior Raymond Marcellin, who had been at the job since 1968, had just been replaced by Jacques Chirac after being ousted over another surveillance scandal – the so-called "Watergoof" (or *Watergaffe*, in French), when several intelligence officers were caught installing bugs in the new headquarters of the investigative journal *Le Canard Enchaîné*in December 1973. In Parliament, where the issue of surveillance was gaining traction (Errera 2003), opposition parties had quickly reacted to this event by calling for an investigatory committee to look into wiretaps conducted by intelligence agencies (Schifres 1973).

Transnational dimension: At the international level too, the risk entailed by new technologies for privacy and other civil rights as well as the legal means for addressing these risks became a focal issue for international organisations like the United Nations, the Council of Europe or the OCDE (Fuster, 2015:76).

Change in oversight (conditions, effects): At the time, the memory of World War II and of the abuse of the Vichy government were still vivid among French elites, and *Le Monde*'s disclosure and the wider context led to profound change in oversight. Facing a growing scandal, the government chose to withdraw the plan and went on to commission a report on the protection of civil rights in the age of computing. The so-called Tricot report, published in 1975, voiced what had by then become widespread concerns: "By reinforcing the means of the government to track, analyse and expose various human activities," the report stressed, "computers go in the direction of technical efficiency but not that of liberty" (Tricot 1975). The following year, the French data protection law – the so-called loi "informatique et libertés"– was adopted by the Parliament, establishing a data protection authority with significant powers on both public and private databases – although in the name of "national security," those of intelligence services remained largely out of its reach. The same year, the first "Freedom of Information Act" was also adopted and presented as a way to ramp up safeguards against the abuse of government secrecy.

References

Errera, R. (2003). Les origines de la loi française du 10 juillet 1991 sur les écoutes téléphoniques. *Revue Trimestrielle Des Droits de l'Homme*, *55*, 851–870.

Fuster, G. G. (2014). *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Springer Science & Business.

Heilmann, E. (2005). Le désordre assisté par ordinateur: L'informatisation des fichiers de police en France. *Les Cahiers de La Sécurité. Revue Trimestrielle de Sciences Sociales*, *56*, 145–165.

Tricot, B. (1975). *Rapport de la commission informatique et libertés (décret n° 74.938 du 8 novembre 1974)*. La Documentation française.

Media archives

Boucher, P. (1974, March 21). Une division de l'informatique est créée à la chancellerie " Safari " ou la chasse aux Français. *Le Monde*. https://www.lemonde.fr/archives/article/1974/03/21/une-division-de-l-informatique-est-creee-a-la-chancellerie-safari-ou-la-chasse-aux-francais_3086610_1819218.html

Le Monde. (1972, November 15). Le SDECE entreprend d'améliorer le recrutement et de moderniser ses matériels. *Le Monde*. https://www.lemonde.fr/archives/article/1972/11/15/le-sdece-entreprend-d-ameliorer-le-recrutement-et-de-moderniser-ses-materiels_2397800_1819218.html

Schifres, M. (1973, December 17). L'Assemblée nationale refuse par 258 voix contre 217 de constituer une commission d'enquête sur les écoutes téléphoniques. *Le Monde*. https://www.lemonde.fr/archives/article/1973/12/17/l-assemblee-nationale-refuse-par-258-voix-contre-217-de-constituer-une-commission-d-enquete-sur-les-ecoutes-telephoniques_3143621_1819218.html

Collection of TV reports on the SAFARI Affair and the adoption of the French data protection law: https://sites.ina.fr/cnil/focus/chapitre/2/medias

US 1975-12-22: The CIA's CHAOS Scandal and the Church Committee

In late 1974, an investigation published in the New York Times revealed that the CIA had engaged in sustained domestic surveillance efforts in the previous years. When new revelations on the FBI's counterintelligence abuse surfaced a few days later, a new Left-leaning Congress established investigative committees on intelligence oversight, one of which came to be known as the "Church Committee". Despite important and numerous findings disclosed by these congressional efforts, ensuing reforms were limited and arguably helped shield intelligence agencies from the radical and adversarial engagement they had faced since the late 1960s.

Starting point: Just a couple of days before Christmas Eve in 1974, the New York Times published a story by Seymour Hersh, then a young journalist awarded with the Pulitzer Prize for his scoops on the My Lai massacre in Vietnam (Hersh, 1974a). Covering the first page of the December 22nd issue, large prints read: "Huge C.I.A. operation reported in U.S. against antiwar forces [and] other dissidents in Nixon Years" (Hersh 1974). Citing "well-placed government sources", the exposé went on to claim that the CIA, "directly violating its charter" barring it from operating on US soil, had "conducted a massive, illegal domestic intelligence operation during the Nixon administration against the antiwar movement and other dissident groups". In the course of this operation codenamed CHAOS, files had been gathered on 10,000 U.S. citizens. The CIA had also engaged in illegal break-ins, wiretaps, and mail openings. Hersh's article was not his first on the CIA. Three months earlier, he had revealed that the CIA and the state department had lied to congress about their efforts to overthrow Salvador Allende in Chile (Hersh, 1974b) . In some ways, Hersh's revelations about the CIA's domestic spying was old news given that the program had been discontinued. But after years of repeated controversies, the intelligence establishment's support base among political and media elites was stretched thin.

Wider intelligence-related context: Apart from its disastrous operation at the Bay of Pigs in Cuba in 1962, when a U.S. plan to invade Cuba failed, the CIA had for the most part remained out of the spotlight. Still in 1967, Ramparts magazine, a publication paradigmatic of the radical culture of the late sixties, had uncovered the CIA's ties to the National Students Association and its wider efforts at reining in communist and leftist

sympathies on U.S. campuses (de Vries, 2012). Upon taking office in 1973, new CIA director James Schlesinger hadreined in some of the most controversial programs. Shocked and furious to discover in the newspaper that 5 out of 7 of the men involved in the Watergate break-in at the Democratic Party's headquarters had worked for the CIA. Furious, he launched an internal inquiry to document any 'illegitimate' spying and other forms of possible abuse which the CIA might have, or were still engaged in. The report from this inquiry (nearly 700 pages long) that listed these practices became known internally as the list of "family jewels". It is based on this report that Hersh investigated the CIA and published his damning exposés on the CIA in late 1974. Besides operation CHAOS, the "family jewels" included assassination plots, drug experiments, the bugging of journalists, and a mail-opening program.

But the CIA was not the only agency to be exposed. By 1974, the whole of the US intelligence community was on the defensive. Amongst other examples, the 1970 CONUS Intel scandal,the revelations by former NSA analyst Perry Fellwock (pseudonym Winslow Peck) of the NSA's ECHELON program in *Ramparts* magazine, the revelations of the COINTELPRO programs by activists who broke in an FBI field office in 1971, the Watergate discoveries, painted an ugly picture. For many, the world of intelligence appeared to be the prime driver of an authoritarian drift. Trust in the intelligence agencies by the U.S. public was at an all-time low. According to historian Kathryn Olmsted:

> "The proportion of Americans who had a 'highly favourable' impression of the FBI had fallen from 84 percent in 1965 to 52 percent in 1973. In 1975, that figure dropped again to 37 percent. Although the Gallup organisation did not ask Americans about the relatively anonymous CIA before 1973, the agency at that time was held in lower esteem than the FBI: only 23 percent of Americans gave the CIA a highly favourable rating. In 1975, the figure fell to 14 percent. Among college students, the CIA was highly regarded by only 7 percent" (Olmsted, 1996).

And yet, according to Olmsted, after Watergate and the resignation of Richard Nixon, the mainstream press was becoming wary of its own power. Realising that attacking the government could entail big consequences, many editors and journalists felt like it was the time to focus on "nation-healing stories" – an expression coined by producers at CBS. In other words, most of the Fourth Estate was now keen on restoring confidence in the government. Meanwhile, the sitting director of the CIA, William Colby, denied Hersh's allegations and claimed that the CIA operations were not massive. His colleagues blasted the reporter for his article's faint factual basis and supposed exaggerations. At first, it looked as if the New York Times disclosure of the CIA domestic spying would die off. It was only in January 1975, when the Washington Post revealed that now defunct J. Edgar Hoover had kept personal records on congressmen (Kessler, 1975), that the New York Times would state that "the Year of Intelligence" had been launched.

Change in oversight: The political context was in some ways explosive. Many newly elected members of Congress who arrived on Capitol Hill in January 1975 were young and "inexperienced" Democrats. The "screaming Watergate babies", as historian Kalman (2010) referred to them, were supposedly very Left-leaning. Reacting to the recent disclosures, they had run campaigns attacking the "imperial presidency" embodied by Nixon, promising to bring a progressive agenda to Washington.

On New Year's eve, Senator Hubert Humphrey, a former vice president, had announced that new legislation would be introduced to create a permanent Joint Committee on National Security. "The time has come," he said, "for Congress to face up to a responsibility it has shirked for too many years". Congress had already scored important achievements in that regard with the adoption of the Hughes–Ryan Amendment in late 1974, a statute that required the president to approve and report to Congress all important covert actions by the CIA. Riding that wave, on January 27, the Senate voted by near unanimity to establish a 11-member committee to conduct a nine-month, $750,000 operation, with a staff of 135 people, into U.S. intelligence operations. Frank Church, a Democrat from Idaho, would head the committee. The House of Representatives soon followed suit, with what would be known as the Pike committee. Ford's White House also established a blue-ribbon commission headed by the Vice-President, Nelson Rockefeller, to look into alleged CIA abuse, a move widely seen as a way to undercut any aggressive investigation by Congress.

Both investigations represented an unprecedented look at U.S. Intelligence Agencies, including not only the CIA and the FBI, but also the NSA, the Internal Revenue Service, and the Defense Intelligence Agency. Both

committees unearthed many hitherto unknown cases of abuse,e.g. the FBI's blackmailing of Martin Luther King, secret budgets funding sensitive intelligence operations, and serious gaps in executive oversight and chains of command. However, very few of their recommendations saw the light of day. Plans to devise detailed legislative charters for intelligence agencies were abandoned under the Carter administration (Lardner, 1978). Often presented as a sign of the enduring success of the Church investigation, the 1978 Foreign Surveillance Act (FISA) did establish a special secret court (the so-called FISA court), forcing the CIA and FBI to get warrants before engaging in domestic surveillance. But this statute's principles, such as the prohibition on warrantless surveillance and the foreign-domestic distinction would later be undercut, first by Reagan, then by Clinton and finally by Bush. The more ambitious 1975 plans to devise detailed legislative charters for intelligence agencies were abandoned under the Carter administration. Even on the issue of covert assassination by the CIA, the executive branch's ways of reining in this controversial practice has been interpreted as a legal subterfuge (Trenta, 2018). The early 1970s calls for radical reforms coming from the Democratic Party (Blum, 1973) had turned into ancient history.

As for the one other major reform associated with the Church committees – the creation of the permanent select committees on intelligence in Congress – it almost failed to pass when it was put to vote on the Senate floor in early 1976 (Olmsted, 1996). Whilst these committees have been praised by many scholars within Intelligence Studies as the true beginning of democratic intelligence oversight, the reform significantly reduced the number of Congressmen receiving classified information on national security policy. Meanwhile, both Congress and the executive branch began taking steps to halt internal dissent and dissuade whistleblowers to talk to the press or to Congress. This marked the beginning of a process where whistleblowers were confined to the role of "organisational defenders" (Gurman & Mistry, 2020) rather than public advocates against intelligence abuse.

In February 1976, former CIA director William Colby found that the congressional investigations had actually strengthened the CIA by clarifying the boundaries "within which it should, and should not, operate" (quoted in Johnson, 2015). While noting that, by the mid-1980s, the congressional committees on intelligence were "largely staffed by former CIA officials", Olmsted (1996) also quotes many executive branch and intelligence officials who remained unimpressed with the legacy of the Church committee. Reacting to intelligence controversies under Reagan, President Ford's counsel Phil Buschen for instance concluded: "I'm not sure the reform was lasting." Just a few months before the Iran-Contra affair (see below), New York Times reporter Leslie Gelb concluded that congressional oversight had produced "a decade of support" for the CIA. Daniel Patrick Moynihan, former vice chairman of the intelligence committee then told Gelb that, "like other legislative committees, ours came to be an advocate for the agency it was overseeing" (Gelb, 1986).

References

Blum, R. H. (1972). *Surveillance and Espionage in a Free Society* (Report by the Planning Group on Intelligence and Security of the Polity Council). Democratic National Party.

Carmack, B. (2019). My Brother's Keeper : Using the Foreign Intelligence Toolbox on Domestic Terrorism. Mitchell Hamline Law Review, 46, 1122.

de Vries, T. (2012). The 1967 Central Intelligence Agency Scandal : Catalyst in a Transforming Relationship between State and People. *The Journal of American History*, *98*(4), 1075-1092.

Fenske, D. (2008). All Enemies, Foreign and Domestic : Erasing the Distinction between

Foreign and Domestic Intelligence Gathering under the Fourth Amendment. Northwestern University Law Review, 102, 343.

Halperin, M. H., Berman, J. J., Borosage, R. L., & Marwick, C. M. (1976). The Lawless State : The Crimes of the U.S. Intelligence Agencies. Penguin Books.

Johnson, L. K. (2015). *A Season of Inquiry Revisited : The Church Committee Confronts America's Spy Agencies*. University Press of Kansas.

Kalman, L. (2010). Right Star Rising : A New Politics, 1974-1980. W. W. Norton & Company.

Mistry, K., & Gurman, H. (eds.). (2020). Whistleblowing Nation : The History of National Security Disclosures and the Cult of State Secrecy. Columbia University Press.

Townley, D. (2018). Spies, Civil Liberties, and the Senate : The 1975 Church Committee [Phd, University of Reading]. http://centaur.reading.ac.uk/83873/

Trenta, L. (2018). 'An act of insanity and national humiliation' : The Ford Administration, Congressional inquiries and the ban on assassination. Journal of Intelligence History, 17(2), 121-140. https://doi.org/10.1080/16161262.2018.1430431

Turner, S., & Thibault, G. (1982). Intelligence : The Right Rules. Foreign Policy, 48, 122-138. https://doi.org/10.2307/1148270

Media archives

Gelb, L. H. (1986, July 7). Overseeing of CIA By Congress Has Produced a Decade of Support. The New York Times. https://www.nytimes.com/1986/07/07/us/overseeing-of-cia-by-congress-has-produced-decade-of-support.html

Hersh, S. M. (1974a, December 22). Huge CIA Operation Reported in US Against Antiwar Forces, Other Dissidents, In Nixon Years. The New York Times. https://www.cia.gov/readingroom/document/cia-rdp77-00432r000100340001-9

Hersh, S. M. (1974b, September 8). C.I.A. Chief Tells House Of $8-Million Campaign Against Allende in 70–73. The New York Times. https://www.nytimes.com/1974/09/08/archives/cia-chief-tells-house-of-8million-campaign-against-allende-in-7073.html

Kessler, R. (1975, January 19). FBI Had Files on Congress, Ex-Aides Say. The Washington Post.

Lardner, G. (1978). Missing intelligence charters. (No reforms enacted since Congressional investigation). The Nation, 227, 168.

UK 1976-05-01: Outing the GCHQ

In a 1976 article in the Time Out magazine, journalists Duncan Campbell and Mark Hosenball revealed the existence of one of the UK's most secretive intelligence agencies: the Government Communications Headquarters (GCHQ) and its partnership with the US National Security Agency (NSA). The article revealed the extensive surveillance practices of the GCHQ as part of a UKUSA agreement, which did not spare friends or allies. The revelation of GCHQ's existence is particularly important as scandals emerged in the wake of secret services reactions to the article: placing Campbell under surveillance, deporting his co-author, trying to prosecute him under the Official Secrets Acts and finally prosecuting him in the so-called ABC case in 1978. This case is particularly important to highlight the role investigative journalists have played in publicising the activities of intelligence agencies and raising questions of democratic accountability.

Starting point: In May 1976, an article entitled 'The Eavesdroppers' was the first to speak publicly about GCHQ, the UK's signals intelligence agency, and to outline its wide-ranging surveillance activities and locations across the country. Duncan Campbell and Mark Hosenball argued the so-called Five Eyes (electronic intelligence agencies in the US, UK, Australia, Canada and New Zealand) had 'divided the monitoring of the world's communications between them' (Campbell and Hosenball 1976). The article did not only reveal the extent and growing importance of the electronic communications for intelligence agencies, but also that British and American private companies were given lucrative contracts by the GCHQ. In the wake of the article's publication, the government attempted to prosecute Campbell under the Official Secrets Act. Yet, he could not be found to have violated the Official Secrets Act, as the information he had used was publicly available. Campbell recounts having stumbled across a GCHQ location as a child roaming the countryside. Later on, he explains that, '[a]t the public library, I checked every phone book in the country, looking for more sites with the same name' (Campbell 2015b). Campbell checked for"CWOS", which stood

for “Composite Signals Organisation Station” (Campbell 2015a). However, the government ordered the deportation of his co-author, US citizen Mark Hosenball (Stephenson and Campbell 2017).

Following the publication of the article, Campbell was contacted by a former Intelligence Corps corporal, John Berry, who was ready to provide further details about GCHQ activities in Cyprus. After Campbell and *Time Out* journalist Crispin Aubrey met Berry, they were all detained for breaching the Official Secrets Acts. The so-called “ABC” trial ensued, which was named after the initials of the three men accused of espionage and of breaching the Official Secrets Acts. Most of the charges were ultimately dropped. The trial attracted a lot of public attention and mobilisation. Historian Richard Aldrich (2010) recounts that an “ABC Defence Committee” was set up to support the defendants. The committee organised a march in Cheltenham demanding that charges against the three be dropped.

Wider intelligence-related context: The publications and scandals concerning GCHQ happened in the wake of the Church Committee and investigations into the illegal activities of the CIA. As Paul Lashmar (2020: 133) explains, “British journalists read the *Washington Post* and *The New York Times* daily and asked, what is the British SIS angle on the latest revelations of US intelligence wrongdoing?” It is in this wider context of lack of accountability, abuse and secrecy – as well as revelations and investigations – that the *Times Out* article was published. Campbell’s articles and books started to paint a picture of the surveillance activities of GCHQ in Britain, as well as collaboration with the US National Security Agency. The public discourse that SIGINT surveillance was not conducted in peacetime had been shattered. Questions of illegal activities and lack of accountability became an increasing concern. However, Campbell and his associates became targets of surveillance and repression. As an article in *The Guardian* put it almost a decade after the publication of “The Eavesdroppers”:

To write about the world of espionage is still, in England, the act of a brave man. Our fearsome and absurd laws not only mean that accurate information about this “missing dimension” to political life is hard to come by, but that those who do come by it are liable to court action and house searches (Duncan Campbell) or even to extra legal deportation (Johnathan Bloch) (Johnson 1984).

Transnational dimension: One of the key elements that emerged from Duncan Campbell’s research on the GCHQ and the NSA was the extent to which satellite stations were used to ‘spy on mainland commerce and politics, either for the benefit of the US and the UK – or even the US alone’ (Campbell 1998, 46). “The Eavesdroppers” had revealed the partnership between the GCHQ and the NSA, and discussed the cooperation between the so-called “Five Eyes”. The prosecution of the journalists under the Official Secrets Acts also showed that piecing together information from public sources and whistleblowers was key to public debates and oversight.

Change in oversight: The ABC trial and the publication of “The Eavesdroppers” did not lead to immediate changes in oversight. Campbell recalls that, when detained under the Official Secrets Act, he thought “this was a hustle”, as a parliament commission recommended that the Official Secrets be changed (Campbell 2015). The deportation order for Mark Hosenball and Philip Agee (a former CIA agent who had published *Inside the Company*, a book about the CIA) under the Immigration and Nationality Act 1971 led to a debate in the House of Commons about freedom of the press. The debates raised questions about the different treatment of UK citizens and non-citizens and the use of immigration legislation to deport foreigners who had not been accused of any crime. Most importantly, Labour MPs were concerned that the Home Secretary took this decision without making some of the evidence available. A refusal to reveal evidence has been used throughout history to perpetuate injustice and to conceal the truth” (Stanley Newens in House of Commons 1977, col 377). In his “authorised” history of the GCHQ, John Ferris advances an opposite view, arguing that ‘Whitehall and its opponents drove Britain down a road of scandal, which ultimately made GCHQ a public and trusted institution’ (Ferris 2021). While Ferris is right about the “road of scandal”, his assessment of the GCHQ as a “public and trusted institution” remains controversial. Actually, the road of scandal continued well beyond the 1970s.

The scandals that revealed what was effectively an open secret – the existence of the GCHQ – also show the importance of the press, journalists and public mobilisation in holding the secret services accountable and promoting public understanding about surveillance activities. As Aldrich notes, the revelations about

GCHQ and SIGINT practices in peacetime 'inspired radical campaign groups to begin "watching the watchers"' (Aldrich 2010, Loc 5840).

References

Aldrich, Richard James. 2010. *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency*. London: Harper Press.

Ferris, John. 2021. *Behind the Enigma: The Authorised History of GCHQ, Britain's Secret Cyber-Intelligence Agency*. London: Bloomsbury.

House of Commons. 1977. "Mr Agee and Mr Hosenball 1977 Accessed 9 November 2021, https://hansard.parliament.uk/Commons/1977-05-03/.

Johnson, RW. 1984. "Books: Looking at Spies with a Critical Intelligence / Reviews of Recent Books on Espionage". *The Guardian*, 27 December.

Lashmar, Paul. 2020. *Spies, Spin and the Fourth Estate: British Intelligence and the Media* (Edinburgh: Edinburgh University Press).

Media archives

Campbell, Duncan, and Mark Hosenball. 1976. "The Eavesdroppers." *Time Out*, 21 May, https://www.duncancampbell.org/PDF/1976-may-time-out-the-eavesdroppers.pdf, Accessed 28 April 2022.

Campbell, Duncan. 1998. "Listening in Silence." *Index on Censorship* vol. 5:46-53.

Campbell, Duncan. 2015a. "My Life Unmasking British Eavesdroppers." The Intercept 2015 Accessed 8 November 2021, https://theintercept.com/2015/08/03/life-unmasking.

Campbell, Duncan. 2015b. "GCHQ and Me", Open Democracy, https://www.opendemocracy.net/en/opendemocracyuk/gchq-and-me/ (Accessed 19 May 2022).

Stephenson, Lorna, and Duncan Campbell. 2017. "Uncovering the Secret State (21 November) 2017 Accessed 29 October 2021, https://thebristolcable.org/2017/11/uncovering-secret-state/.

DE 1977-2-27: The Traube Scandal

Klaus Traube was a top-manager in the nuclear sector who became a notable critic of the technology of nuclear energy. His advocacy – as suspected ties to far left groups – led him to be put nuder surveillance by the domestic intelligence service of Germany, the Bundesamt für Verfassungsschutz (BfV). Once the operation was revealed in the media and the accusations of complicity with anarcho-leftist scene proven false, the scandal led to the resignation of the Interior minister and the expansion of the powers of the parliamentary intelligence oversight body with the adoption of the 1977 Act on Parliamentary Control of Federal Intelligence Activities.

Starting point: In February 1977 *Spiegel* published a story on an illegal surveillance activity of the BfV. The article dealt with Karl Traube's case, a victim of illegal and unauthorised wiretapping and bugging due to false allegations of him being a member of the Red Army Faction (RAF). The case became public when documents from the authorities were passed on by Karl Dirnhofer, a civil servant at the BfV, to the journalist Hans Georg Faust, who forwarded the papers to the news magazine ER *Spiegel*. There was a continuous covering of the issue in the German media.

Wider intelligence-related context: In the 1970s Klaus Traube had moved from being a top manager in the nuclear energy industry to an avowed opponent of this form of energy. After this change of views, he came into the focus of the BfV, which assumed that this change was due to a radical leftist connection, and more specifically organization RAF. On 30th December 1975, the BfV launched an extensive eavesdropping operation, not covered by the laws of the time, by installing bugging devices in the home of Traube. They also gave a recommendation to his employer who, as a result, dismissed him. In the Winter of 1976 the BfV broke into his house again to remove the devices. The then federal Minister of the Interior knew of the operation

and had, at least non-explicitly, approved of it. In the words of *Spiegel*, intelligence agencies "broke into the apartment of a nuclear scientist they suspected and installed an electronic 'bug' " (Spiegel, 1977a). According to the article, "the head of the Office for the Protection of the Constitution, Meier, approved the 'eavesdropping attack' and the Minister of the Interior, Maihofer, knew about it." (Spiegel, 1977a). The only thing that could evidently be said was that Traube had personal contact to some individuals of the anarcho-left scene, many of them via the communist lawyer Inge Hornischer, who was Traube's former neighbour in 1967 and whom he consulted regarding his divorce.

Change in oversight: As Seifert (1977) shows, the public uproar was significant. The scandal led to the resignation of the then Minister of Interior Maihofer in 1978. The "whistleblowers" were charged with betrayal of secrets. Dirnhofer's main trial was not opened because the evidence presented for his conviction also originated from illegal telephone surveillance. Faust's main trial was opened, but he was acquitted by the Bonn Regional Court. Furthermore, it is suggested that this scandal led to the adjustment of the "Parlamentarische Vertrauensmännergremium" (PVMG), which was the first parliamentary oversight body of the early Federal Republic of Germany. The former PVMG was viewed as relatively toothless and ineffective. Consequently, it was upgraded to the "Parlamentarische Kontrollkomission" (PKK) with the Act on Parliamentary Control of Federal Intelligence Activities (NDKontrG a.F.) in 1977. The PKK was responsible for controlling the federal government with regard to the activities of the three services. In contrast to the PVMG, the instruments and competences necessary for this task were legally defined for the first time. As described by Friedel (2018, 265), the act was groundbreaking because "(…) it was the basis for the control architecture as it still exists today, this marked the beginning of the 'actual history of control'.".

References

Friedel, A. (2019). *Blackbox Parlamentarisches Kontrollgremium des Bundestages: Defizite und Optimierungsstrategien bei der Kontrolle der Nachrichtendienste.* Wiesbaden: Springer Fachmedien.

Seifert, J. (1977). Die Abhör-Affäre 1977 und der Überverfassungsgesetzliche Notstand: Eine Dokumentation zum Versuch, Unrecht zu Recht zu machen. *Kritische Justiz*, 10(2), 105-125.

Media archives

Augstein, R. (1977, February 27). *Atomstaat oder Rechtsstaat? Der Spiegel*. *https://www.spiegel.de/politik/atomstaat-oder-rechtsstaat-a-1727e588-0002-0001-0000-000040941939?context=issue*

Der Minister und die "Wanze". (1977, February 27). *Der Spiegel*. *https://www.spiegel.de/spiegel/print/d-40941938.html*

Maihofer: Abgang gesucht. (1978, June 4). *Der Spiegel*. https://www.spiegel.de/spiegel/print/d-40615769.html

Zundel, R. (1977, March 11). *Maihofer – ein Idol ist zerstört*. Die Zeit. *https://www.zeit.de/1977/12/maihofer-ein-idol-ist-zerstoert/komplettansicht*

FR 1983-09-30: The Elysee Cell, the Left and the National Security State

On 1983 September 30th, Le Monde *quoted high-ranking sources alleging the creation of a parallel intelligence unit at the Elysée Palace, then under the tenure of socialist president François Mitterrand, tasked with the extra-legal surveillance of journalists, lawyers, businessmen, and politicians. The scandal would only burst in the early 1990s when what became known as the "Elysée Cell" drew the attention of journalists and lawmakers. It marked the first of many revelations of intelligence abuse under a centre-Left government and played a key role in the adoption of the first piece of legislation regulating surveillance activities: the Wiretap Act of 1991.*

Starting point: In an article published on September 30th 1983, *Le Monde* described "several reliable reports – denied by the Élysée Palace" of phone tapping, particularly of journalists, conducted outside the scrutiny of

the executive agency charged with overseeing the administrative wiretapping approved by the government. The author of the piece, Edwy Plenel, reported that fourteen police officers from domestic intelligence services had joined this "Elysian cell" led by close allies of President François Mitterrand. Its premises were "located in a discreet villa on the rue de l'Élysée, where on the second floor there are a number of offices repainted without any distinctive sign as well as computer terminals", Plenel wrote (2006). As the press would later find out, those PCXT computers ran IBM software by the names of "Filing" and "Reporting" (Pontaut 1996, Plenel 2006).

Wider intelligence context: The election of President François Mitterrand in May 1981 meant that it was the first time in almost 50 years that the Left had its grip on the executive and the legislative branches of government. The new political and administrative personnel came in with a strong distrust of intelligence agencies. The intelligence agencies' notorious anti-communism and interference in political affairs in the past decade (including suspicion of political assassination of leading Lefist activists Henri Curiel (1978) and Pierre Goldman (1979)) – had made it a clear adversary to the newcomers. In 1972, the "Common Platform" of the French Left even pledged that the SDECE (France's foreign intelligence service) would be disbanded. From 1973 on, Mitterrand himself had echoed these criticisms, for instance asking for a parliamentary investigation on wiretapping. But in the period leading up to the May 1981 election, the tone of Mitterrand's Socialist Party softened and the first days of its presidency did not seem all that bad for intelligence agencies (Laurent 2015). The nomination of Maurice Grimaud, former prefect of police for Paris during the "events" of May 1968, did much to ease the relationships with the world of intelligence.

However, in the vein of Grimaud's liberal vision for police reforms, the socialist government seemed followed up on its promise to reform intelligence. In July 1981, the government nominated a high-ranking judge to head a committee tasked with proposing a detailed legal framework around wiretapping. In Parliament, the Communist Party asked for and succeeded in the creation of an investigative committee on the Service d'Action Civique (SAC), a parallel intelligence organisation set up in 1960 under the presidency of Charles De Gaulle that was suspected of operating closely with official intelligence and of dealings with organised crime.

In August of that year, Prime Minister Pierre Mauroy asked a Member of Parliament and member of the Council of State Jean-Michel Belorgey to write a study on police reform. The draft report, handed out in January 1982, came out strongly against the leading domestic intelligence agency, the Direction de la Surveillance du Territoire (DST). "The argument of classification is truly a difficult one to evade," Belorgey contended (quoted in Laurent 2015). "The DST," he went on "is, in reality, the sole master of the definition of its own strategies, of the ethics it sees fit and of the legitimacy of the freedom that it grants itself in the name of patriotic defence but also, and less praiseworthy, in relation to legality and the republican tradition."

Yet, calls for reforms did not materialise, and the recommendations of liberal reformers were postponed to a later date. In the meantime, the Socialist Government reasserted the role of domestic intelligence agencies. A wave of terrorist attacks were used to further entrench their role and the government chose to veil in secrecy the overhaul of intelligence databases in 1986. By then, the Council of State had also sheltered intelligence files from Freedom of Information Requests and the CNIL – the Data Protection Authority – appeared to be fighting an upward battle in exerting oversight in these matters (Plenel 1990).

Despite Plenel disclosure in 1983, the scandal of the Elysée Cell – finally disbanded in 1988 – would only unfold from 1992, when the national press published the testimony of Paul Barril, one of its key players. In turn, this disclosure led to the first legal challenge by Edwy Plenel, one of the journalists spied upon by the cell, along with about 150 individuals. The judicial investigation stumbled upon state secrecy, and the trial only began in 2004. Judges acknowledged that although the Elysée Cell was illegal, so were all wiretaps conducted by intelligence agencies, given the lack of any detailed legal framework. By then, a series of intelligence scandals had helped rebuild the case for reform. The government came under huge pressure, especially after the Rainbow Warrior affair in 1985, when the foreign intelligence agency (reorganized in 1982 and renamed DGSE (for Direction Générale de la Sécurité Extérieure)) bombed and sank a Greenpeace ship that was mobilising against France's nuclear trials in Polynesia. One member of the crew was killed and Prime Minister Laurent Fabius swore that change was in order: "A large country needs intelligence services.

At the same time, they need to be subject to control" (Le Monde, 1985). The DGSE, however, was merely reorganised and the chains of command and control with other parts of the executive reinforced (Silberzahn, 2016).

Transnational dimension: The European Court of Human Rights sparked the process of legalising f intelligence surveillance in France. In the late 1980s, important criminal cases regarding the French legal framework for government surveillance reached the ECHR. In two unanimous decisions issued in April 1990, the Court struck down on French wiretap warrants given that they were not carried out "in accordance with the law."

Changes in oversight: In response to these condemnations, the government moved quickly to enact a statute covering both judicial and administrative wiretapping of correspondences," i.e, the content of private communications. After only forty days of legislative debates, Parliament passed the Wiretapping Act of 1991. From then on, judicial wiretaps could only be ordered by the investigatory magistrate, when necessary, and only for serious crimes punishable with more than two years of imprisonment. In addition to this, the Act introduced many procedural safeguards such as written decisions, record-keeping, and special protections for lawyers. As for administrative wiretaps conducted by intelligence services on French territory (which the law termed "security interception"), these could only be allowed "exceptionally" and for the following goals: national security, the safeguarding of France's "scientific and economic potential", the prevention of terrorism, the prevention of organised crime and of the formation of extremist groups and militias that had previously been dissolved (in accordance with a 1936 law against fascist leagues). Wiretap authorisations were also issued under the authority of the Prime Minister for a renewable 4-month period.

Finally, an administrative oversight commission was established: the Commission nationale de contrôle des interceptions de sécurité (CNCIS), it comprised of nine members, mixing judges and members of Parliament in one body. The Prime Minister had to notify the CNCIS of every wiretap authorisation within 48 hours. If the CNCIS deemed the authoriz=sation illegal, it could send "recommendations" to the Prime Minister to ask for the wiretap to end. Within a year, it became standard practice for the Prime Minister to wait for the CNCIS opinion before conducting wiretaps. Authorisations remained valid for four months, after which they either had to be renewed or else expire. The Act's article 20 also granted a blank check to the DGSE to intercept wireless communications.

The creation of the CNCIS meant yet another extra-judicial oversight agency dedicated to activities of state surveillance. Whilst some had called for a powerful entity overseeing all surveillance activities by the state, the government chose to fragment oversight, creating a weak agency bound to secrecy.

References

Laurent, S.-Y. (2015). Face aux « services » (1981-1983): Une autre leçon pour la gauche au pouvoir ? Histoire@Politique, 27(3), 62–73.

Silberzahn, C. (2016). Les mutations de la DGSE après la crise du Rainbow Warrior. Apres-demain, 37(1), 15–17.

Plenel, E. (2006). *Le journaliste et le Président*. Stock.

Pontaut, J.-M., & Dupuis, J. (1996). *Les Oreilles du Président* (Fayard édition). Fayard.

Media archives

'Texte du Premier Ministre "Je ne dispose, à ce stade, d'aucun élément me permettant de contredire la conviction de M. Tricot"'. (1985, August 29). *Le Monde*. https://www.lemonde.fr/archives/article/1985/08/29/le-texte-du-premier-ministre-je-ne-dispose-a-ce-stade-d-aucun-element-me-permettant-de-contredire-la-conviction-de-m-tricot_3049395_1819218.html (December 12, 2021).

Plenel, E. (1990, March 15). La nécessité d'un contrôle. *Le Monde*. https://www.lemonde.fr/archives/article/1990/03/15/la-necessite-d-un-controle-par-edwy-plenel_3956707_1819218.html

US 1986-11-3: Reagan's Iran-Contra Affair

The Iran-Contra scandal exposed the US selling arms to Iran, and diverting funds from these sales to arm the Contras, a right-wing militant group in Nicaragua. In contravention to its own embargoes and global campaigns, the US had been supplying weapons to Iran and using the profits to fund the Contras, at a time when Congress had prohibited the arming of the Contras via a series of legislative amendments known as the Boland Amendment. The scandal, considered hugely underreported relative to its magnitude, and in comparison to other scandals like Watergate, provides insight into the violent and visible consequences of intelligence. It also exposed the very visible circumvention and shortcomings of official oversight through the destruction of evidence, and through the elasticity of legislation.

Starting point: There are two significant events commonly cited as starting points. One is the publication of a piece in the Lebanese magazine *Ash-Shiraa* by Iranian Revolutionary Guard Mehdi Hashemi on the 3rd November 1986. Hashemi revealed the selling of US weapons to Iran at a time when the US had declared an arms embargo on Iran and launched 'Operation Staunch' demanding from other states not to supply military equipment and arms to Iran. Although the US had suggested it was on hostile terms with Iran after the revolution and the hostage crisis of 1979 and its proclaimed arms embargo, it had continued selling arms to Iran from the early 1980s. Given that Iran had previously been the US's largest arms buyer, the US feared that a lack of US "support" would change Iran's dependency towards the Soviet Union who would then have a stronger geopolitical hold, particularly given that the Soviet-Afghan war had started.

Like Iran, Nicaragua experienced a revolution in 1979 that overthrew the violent and US-backed FDN (also commonly known as the Contras). And similarly, the US worried about greater dependency on the Soviet Union, and the rise of socialism as was evident in their assassination and overthrow of Allende in Chile, and Operation Condor initiated by US-backed and trained Augosto Pinochet. A month before the publication in Ash-Shiraa, in October 1986, a Nicaraguan teenager shot down a CIA plane carrying artillery destined for the right-wing rebel group the FDN/Contras. Soon, it was revealed in great detail that the US was funnelling and diverting funds made from its arms sales to Iran to fund the Contras in Nicaragua contravening its own arms embargoes and circumventing various domestic and international laws, using shell companies that filled the pockets of arms dealers, contractors, politicians across various states.

Wider intelligence: Much of the scandal has focused on the role of specific individuals, particularly the US National Security Council staff member Oliver North, North's secretary Fawn Hill, National Security Advisors John Pointdexter and Robert McFarlane, and also figures such as the then president Ronald Reagan, and vice-president George H. W. Bush. Many of the individuals played significant roles in previous wars like Vietnam, in 'secret wars' like in Cambodia and Laos, in intelligence, and many would later play a significant role in defence, intelligence and the wars that followed. Other notable figures in the US include Colonel Robert Dutton, former US Air Force General Richard Secord (who ran the main company linked to the scandal (Enterprise)), founding member of the CIA General Singalub, CIA director William Casey, and Defense Secretary Caspar Weinberger.

The web of intelligence included the actors mentioned above, and was revolving, in that many of these actors interchanged/extended into the private sector, which as Miller suggests, could be seen as tool of secrecy itself - "without anyone being able to prove that the US government was involved" (Miller, 2020, p.115). Similarly, Oliver North's role in diverting funds became a diversion for the scandal itself, with North himself stating in his memoirs: "This particular detail was so dramatic, so sexy, that it might actually—well *divert* public attention from other, even more important aspects of the story,"..."such as what the President and his top advisors had known about and approved" (Kornbluh, 2011 and Byrne, 2015).

The destruction of evidence was a key part of the scandal. North's secretary, Fawn Hill testified in the Congressional Investigation to smuggling classified documents in her clothing and shoes, and Oliver North's destruction and hiding of documents in November 1986. The refusal to acknowledge and provide information was seen in Reagan's testimony where he claimed that he didn't remember over and over again, and in the destruction of the possibly only copy of the presidential order by Pointdexter. This destruction of evidence and of traces is not only seen in the use of shell companies, but in the testimonies of key actors.

Upon Contra leader Calero's receiving of an extra $20 million deposited in the "usual account" from an unknown source, Miller documents North's correspondence and instructions: "'destroy this letter after reading…Please do *not* in any way *make* anyone aware of the deposit…. Too much is becoming known by too many people…We need to make sure that this new financing does not become known….The Congress must believe that there continues to be an urgent need for funding'" (Miller, 2020, pp. 120-121).

Although Iran-Contra showcased the very visible ways in attempting to hide and destroy information, it is worth noting the systemic exemptions that hid and legitimised these violent practices. For example, exemptions from mechanisms like the Foreign Corrupt Practices Act (FCPA) were in place in the name of 'national security'. Under the advise of the CIA, any company which the CIA suggests has a national security role, is exempt from informing the Securities and Exchange Commission (SEC) about foreign payments - making "the massive payment of bribes to facilitate the Iran-Contra fiasco...exempt from the jurisdiction of the FCP'" (Feinstein, 2012, p. 278). Raegan would later assert that "support for freedom fighters is self defence and totally consistent with the OAS and UN Charters" (AP Archive, 1986). Similarly North and Hill in their testimonies would be adamant that their destruction of evidence was for purposes of "national security", and Pointdexter would be adamant to blatantly withhold information in the Iran-Contra hearings.

Transnational: This scandal is evidently a transnational one given the arming of both the Iranian state and the Contras. However, the transnational elements of the scandal reach much wider, and it is precisely through these elements that the contradictory and violent dynamics of intelligence are made clear. As suggested above, the scandal cannot be seen in isolation from ongoing US foreign policy in both Central and South America, and the Middle East, nor taken out of the context of the 'Cold' War.

Feinstein (2012) highlights the crucial role that both Saudi Arabia and Israel played in the scandal. Whilst organising the arrangement for funnelling funds made from arms sales to Iran, to the Contras upon the withdrawal of Congress's support , the US depended on Saudi Arabia, amongst others to act as intermediaries to ensure that the Contras were armed and funded: "After meeting with McFarlene and the Defense Secretary, Caspar Weinberger, Bandar ensured that the Contras received $1m a month from mid-1984. At a breakfast meeting with Reagan in early 1985 King Fahd offered to double the remittances" (Feinstein, 2012, p. 51).

Iranian arms dealer Manucher Ghorbanifar, and billionaire arms dealer Adnan Khashoggi would be the vessels in which Iran approached Israel for arms from the US. Israel was used as the go-between, before the US government would later deal directly with Iran (at the same time it was providing intelligence and monetary support to Saddam Hussein). Statesmen, businessman, governments, and accounts in places ranging from Brunei, Liechtenstein, Panama, Poland, Portugal, and Switzerland were also involved, and to further scandals such as transfer of funds, misdirected funds, and movement of huge arms purchased by North's front company Enterprise, that would later become unnecessary given the lifting of the arms embargo on the Contras (leaving him and his aides to convince the CIA to cover the costs).

The role of shell companies and flow of capital of course necessitated the involvement of transnational actors. Transnational elements were also important in (the clearly linked) military strategy and assistance, including the Brits at the El-Salvador base that British mercenary David Walker was paid for (Miller, 2020). The GTM shell company set up by US intelligence became the source of arms by which the CIA trained the Contras (Feinstein, 2012, p.379). By "transferring surplus NATO equipment from Europe to Israel to replace the Isareli arms that were to be sold to Iran at prices significantly higher than their true market value, the US could use the profits to finance the Contras" (ibid, pp. 379-380). Whilst Israel was supplying arms past their sell by dates to Iran, the US was providing it with supplements, and it was directly supplying arms to the Contras for additional profit (ibid, p. 380). London and New York would be staging grounds for the selling of these weapons.

These small glimpses provide little insight into the countless deaths and violence caused and exposed by such a scandal that fuelled and profited from long wars and massacres like the Contras wars and the Iran-Iraq war. The most prominent and important transnational aspect was the death and destruction caused - amongst factions, sometimes at war with each other but funded and armed by the same network of dealers, and its intermediaries.

Changes in oversight: Soon after Reagan's initial statement on the affair in November 1986, he commissioned the Tower Commission which 'investigated' key figures of the scandal (including the President) and published a report in February 1987, condemning the role of the NSC in the scandal and criticising his lack of supervision/knowledge (conveniently distancing him through his supposed ignorance of the affair). More widely recognised, was the role of the Joint Congressional Committees who held the infamous Iran-Contra hearings from May – August 1987, and published a lengthy report (which within it included a minority report) in November 1987. Later, in the early 1990s Independent Counsel Walsh was appointed to investigate criminal liabilities.

However, even with these various formal oversight mechanisms, some with very public elements like the televised hearings, there was arguably little/no change or accountability. Oversight in this scandal arguably served as a distraction from its violence, and legitimised some of the most problematic parts of it, through leaving areas unquestioned, excluding actors and information, and decontextualising the scandal.

In terms of the formal mechanisms, Kornbluh highlights the exclusion of opponents to Reagan's Contra policy in the setup of the committees (Kornbluh, 1988, p.130). This worked hand in hand with the de-contextualisation whereby the scandal "appears falsely to be an aberration" (ibid, p.132).

Important to note was that criticism of the Joint Committees through its own Minority Report, reinforced the view that the scandal was an aberration:

> "The bottom line, however, is that the mistakes of the Iran-Contra Affair were just that — mistakes in judgement, and nothing more. There was no constitutional crisis, no systematic disrespect for 'the rule of law,' no grand conspiracy, and no Administration-wide dishonesty or coverup. In fact, the evidence will not support any of the more hysterical conclusions the Committees' Report tries to reach."

Meanwhile, the systemic role of covert operations in US foreign policy was ignored, and in fact supported through the accepted premises. This fared terribly, even in comparison to previous oversight mechanisms such as the Church Committee of the 60s and 70s.

The scandal was hugely individualised in the way it was 'dealt with' and reported, with a focus on the role of actors like Oliver North who became the face of the fiasco. Even criticisms of the hearings that have highlighted a much more active role on the part of the Executive/President, have reproduced a focus on the role of individuals. Similarly, as pointed out by Vaughan (2017), challenges by Congress were focused on the tension between executive and legislative actors, rather than the violence ensued by the scandal across the world.

It should also be noted that even with this individual framing/understanding of the scandal, there was little accountability. Impeachment of the president was dismissed given that his presidency was coming to an end. Many of the actors involved were pardoned by George H. W. Bush during his presidency that followed, and who had distanced himself even with his own acknowledgement of knowing the full details, and meetings with Israel's counter-terrorism advisor, Nir. Plausible deniability was embraced, and the approach of refusing to engage was widely adopted by different actors, whether that be a reference to 'memory loss' or outright refusals from, for example, Margaret Thatcher in questions related to the role of the British mercenary group Keenie Meenie Services and David Walker (Miller, 2020).

Arguably, the very exposure to the absences and failures of these oversight mechanisms, can provide a different oversight. The scandal itself tested the formal oversight mechanisms put in place, with a terrible verdict.

Worth acknowledging also is informal oversight mechanisms. One that could be described as such was the protest at the public hearing in 1987, whereby two protestors unfurled a banner that read "Ask About Cocaine Smuggling" and shouted about the death of non-combatants and drug trafficking (L.A. TIMES Archives, 1987), significantly absent from the scandal and its aftermath. Other less formally acknowledged forms of oversight include the persistent asking of information and documents to be released by campaigners,

researchers and organisations over the decades, and the publication of these materials on archives like the National Security archive and Unredacted.

References

Fallis, D. S. (1991). Not the America I Knew. *CovertAction Information Bulletin*, *New World Order: Tunnel at the End of the Light*(37), 42–46.

Feinstein, A. (2012). *The Shadow World: Inside the Global Arms Trade* (revised and updated edition). Penguin Books.

IRAN CONTRA AT 25: REAGAN AND BUSH 'CRIMINAL LIABILITY' EVALUATIONS - National Security Archive Electronic Briefing Book No. 365. (2011, November 25). The National Security Archive. https://nsarchive2.gwu.edu/NSAEBB/NSAEBB365/index.htm

Iran-Contra: Reagan's Scandal and the Unchecked Abuse of Presidential Power. (2015, January 28). https://www.youtube.com/watch?v=xUu8f9rBh_g

Kasper, D., & Trent, B. (Directors). (1988, June). *Cover Up: Behind the Iran Contra Affair*.

Kornbluh, P. (1987). The Iran-Contra Scandal: A Postmortem. *World Policy Journal*, *5*(1), 129–150.

Miller, P. (2020). *Keenie Meenie: The British Mercenaries Who Got Away with War Crimes*. Pluto Press.

The Eugene Hasenfus Story. (1991, February 21). In *PBS WISCONSIN DOCUMENTARIES*. PBS. https://www.pbs.org/video/wpt-documentaries-eugene-hasenfus-story/

Vaughan, D. (2017a, January 11). Dark Shadows: Iran-Contra, Secret Wars & Covert Operations, Part 1. *WhoWhatWhy*. https://whowhatwhy.org/politics/government-integrity/dark-shadows-iran-contra-secret-wars-covert-operations-part-1/

Vaughan, D. (2017b, January 25). Dark Shadows: Iran-Contra, Secret Wars & Covert Operations, Part 2. *WhoWhatWhy*. https://whowhatwhy.org/politics/government-integrity/dark-shadows-iran-contra-secret-wars-covert-operations-part-2/

Vaughan, D. (2017c, February 9). Dark Shadows: Iran-Contra, Secret Wars & Covert Operations, Part 3. *WhoWhatWhy*. https://whowhatwhy.org/politics/government-integrity/dark-shadows-iran-contra-secret-wars-covert-operations-part-3/

Media archives

AP Archive (Director). (1986, November 3). *NICARAGUA reprise (GNS G12118607)*. https://www.youtube.com/watch?v=ttvRTSCsxj4

Kornbluh, P. (2011, November 25). The Iran-contra scandal, 25 years later. *Salon*. https://www.salon.com/2011/11/25/the_iran_contra_scandal_25_years_later/

Schwarz, J. (2018, May 12). OLIVER NORTH WORKED WITH COCAINE TRAFFICKERS TO ARM TERRORISTS. NOW HE'LL BE PRESIDENT OF THE NRA. *The Intercept*. https://theintercept.com/2018/05/12/oliver-north-nra-iran-contra/

THE IRAN-CONTRA HEARINGS : Two Protesters Seized in Outburst. (1987, July 10). *Los Angeles Times*. https://www.latimes.com/archives/la-xpm-1987-07-10-mn-1966-story.html

UK 1987-01-18: The Zircon Satellite Affair

Zircon was the name of an 'exceptionally secret' UK SIGINT satellite project being developed under the conservative government. The existence of the project, and the fact that its 500 million GBP cost had been concealed from Parliament, was revealed by investigative journalist Duncan Campbell. Originally intended to be disclosed by Campbell in a BBC TV documentary, the BBC Director General was persuaded by GCHQ not to air the episode on the grounds of national security. In January 1987 however, the Observer newspaper leaked the

story, under the headline "BBC gag on £500 million defence secret" (Wilby 2006). Campbell then published a detailed account of the Zircon project, the bypassing of Parliament and the BBC censorship, in a New Statesmen article a few days later.

Starting point: On January 18th, 1987, under the headline "BBC gag on £500 million defence secret," The Observer broke the news that the BBC had bowed to government pressure and scrapped a documentary by Duncal Cumbell about the funding of a spy satellite (Observer, 1987). Two years before, in the winter of 1985, Campbell had been commissioned to develop a six-part TV documentary series for BBC Scotland entitled 'Secret Society', about the functioning of the UK Intelligence Community. Campbell's plan was to reveal the existence of the top-secret project to develop a British SIGINT satellite, Zircon, the cost of which had been hidden from scrutiny of the Public Affairs Committee, a powerful Parliamentary watchdog which oversaw government spending (BBC 100, 2022). The satellite was due to be positioned over the Soviet Union, with the capacity to intercept communications in the USSR, Europe and across the Middle East (Campbell, 1987). Campbell was already a well-known whistle-blower on intelligence and security matters, having leaked the existence of GCHQ back in 1976 (Wilby, 2006). The investigative journalist's involvement in the BBC mini-series therefore was a source of great unease in Whitehall, even before the Zircon project was being finalised.

In the run up to Christmas 1985 however, the Director of GCHQ, Peter Marychurch, together with the Secretary of the D-Notice Committee – the government body with the capacity to censor media content on national security grounds –, put pressure on BBC Director General, Alisdair Milne, to axe the programme. After additional persuasion from BBC governors, many of whom had links to the military and intelligence services, Milne complied and shelved the Zircon episode from the 'Secret Society' series. Quickly after the publication by the Observer breaking the story in January 1987, Campbell published an article for the New Statesman. Titled 'Spy In The Sky', it detailed the proposed Zircon project, the bypassing of Parliament and the BBC's so-called 'national security' ban (Campbell, 1987).

Wider intelligence-related context: According to Campbell's sources, four senior defence officials and one former member of GCHQ, the Zircon satellite project mainly revolved around securing the UK's 'status' as a strong power. According to Sir Frank Cooper, former permanent secretary at the Ministry of Defence, and one of Campbell's informants, Zircon was a matter of 'macho politics' (Campbell, 1987). The UK's international standing was firmly intertwined with maintaining a 'special relationship' with the US on nuclear and intelligence policy. SIGINT was crucial in this regard as it would give the UK a 'national capability', eschewing the need to rely entirely on the US for strategic intelligence (Campbell, 1987).

Transnational dimension: The Zircon affair was a story firmly within the geopolitical imaginaries of the Cold War. The shelving of Zircon and the political scandal that ensued revealed that the UK was reliant on the US to practice its full range of SIGINT activities (Ferris 2020: 322). GCHQ biographer John Ferris argues that by the end of the Cold War, GCHQ had fewer resources than its Five Eyes partners, and was less able to adapt to changing circumstances. Unlike the junior partnership that the UK was obliged to enter with the US around nuclear weapons after the collapse of British independent missile programmes however, the relationship with the NSA was slightly more balanced, thanks to the value the NSA placed on GCHQ's data analyses (Ferris 2020: 323). In 1989, Duncan Campbell would reveal that Zircon had been replaced by a U.S ready-made satellite, launched on US Labour Day (4th September 1989), but operating under British control (Campbell, 1989).

Change in oversight: The concealing of the Zircon project from the Public Accounts Committee broke a key agreement between the Ministry of Defence and Parliament. This agreement obliged both the Ministry of Defence and Treasury to inform the Public Accounts Committee about any project which cost above GBP 150 million (Campbell 1987). Reasons of 'national security' were not considered an adequate reason to withhold this information. This agreement was the outcome of the so-called 'Chevaline row', a pact undertaken in 1982 after it was revealed that both Labour and Conservative governments had misled Parliament about a GBP 1 billion project to modernise nuclear warheads – the so-called Chevaline Programme (Campbell, 1987). It can be argued that the Zircon affair directed public attention towards the role of Parliament in holding the spending of intelligence agencies to account. However, as Ferris (2020: 674)

notes, the Zircon affair faded very quickly from the headlines and was perhaps only interesting to the "chattering classes" in any case.

More interesting were the ripple effects that the affair had around discussions of parliamentary privilege and the possibility for whistleblowers to be protected under this privilege. With the Zircon Affair becoming public knowledge, Labour MP Robin Cook organised a screening of Campbell's documentary to MPs in the House of Commons. On the morning of the planned screening, The Attorney General, Sir Michael Havers, requested an injunction in the High Court to block the screening. This was refused, presumably because of the belief of the judge that this matter was for the authorities of the House to deal with (Seaward, 2020). Under further pressure from ministers, the Attorney General argued that the Speaker of the House of commons should prevent the showing of the film, which the Speaker agreed to. Though Campbell tried once again to screen the documentary in the House of Commons, with the help of some opposition MPs, the speaker once again ruled that the programme could not be shown on parliamentary premises. Though copies of the programme had by this time been obtained by many human rights and civil liberties groups which had organised open screenings, The Committee of Privileges reported that the screening would not be protected by parliamentary privilege, hence supporting the Speaker's previous moves to forbid the film being shown within Parliament. Writing on a project on the History of Parliament, Paul Seaward (2020) is clear that this decision reinforced the longstanding principle that "those who chose to send information to MPs – even whistleblowers who were revealing matters that might be of vital significance – were not protected by parliamentary privilege unless they did so as part of a formal proceeding".

References

Ferris, J. (2021). Behind the Enigma: The Authorised History of GCHQ, Britain's Secret Cyber-intelligence Agency. Bloomsbury Publishing.

Media archives

BBC 100 (2022) The Zircon Affair 1986-87. https://www.bbc.com/historyofthebbc/research/editorial-independence/zircon-affair/ Accessed 01/02/2022

Campbell, D. (1987). The Cost of Zircon, New Statesman 27th February 1987: 13-15 . https://www.duncancampbell.org/menu/journalism/newstatesman/newstatesman-1987/The%20cost%20of%20zircon.pdf Accessed 01/02/2022

Campbell, D. (1989) Spy In The Sky, New Statesman 22nd December 1989: 19. https://www.duncancampbell.org/menu/journalism/newstatesman/newstatesman-1983/spy%20in%20the%20sky.pdf

Index on Censorship (1988) The 'Zircon' affair, Index on Censorship, 17:8, 17.

Seaward, Paul (2020) The Zircon Affair, Parliament and the Courts. https://historyofparliamentblog.wordpress.com/2020/05/25/the-zircon-affair-parliament-and-the-courts/

Wilby, D. (2006) The Zircon Affair 1986-87. https://web.archive.org/web/20120905221545/http://www.bbc.co.uk/historyofthebbc/resources/bbcandgov/pdf/zircon.pdf

US 1993-04-16: The Clipper Chip scandal

When in 1993, the US government announced its plan to introduce a new cryptographic standard aimed at facilitating state surveillance by law enforcement and intelligence agencies, it unleashed a wide-ranging mobilisation in favour of privacy. The fight against the "Clipper Chip", as the standard developed by the NSA was called, united a front of rebellious hackers, computer experts, cryptographers, digital rights and human rights groups, industry players and libertarians. Eventually, the Clinton administration had to shelve the plan and liberalise the use of strong cryptography. In the short term, intelligence and law enforcement agencies were defeated but quickly acted to find workarounds to deal with the new realities of pervasive, global digital communications.

Starting point: On April 16 1993, the New York Times revealed a new government plan regarding encryption, to be announced by President Bill Clinton on that day. "The Clinton Administration plans a new system of encoding electronic communications that is intended to preserve the Government's ability to eavesdrop for law enforcement and national security reasons while increasing privacy for businesses and individuals," the article read (Markoff, 1993). It was the U.S. administration's preferred strategy to overcome a controversy that had been raging for years between the world of intelligence and civil libertarians. As journalist John Markoff contended, "the Government has proposed in the past to require the use of a hidden key in the coding hardware or software – a way to crack the code, in other words – to let police security agents decipher messages after obtaining court authorization to do so. Civil liberty concerns aside, computer experts have argued that any such key, no matter how sophisticated, might be figured out by any savvy computer hacker." But now, the government had a solution: "require two separate keys, each to be held by different agencies or organisations". "The new coding devices," the article explained, "will be called Clipper Chips".

Intelligence context: In the early 1990s, around fifteen years had passed since cryptography had escaped the military bottle. In the new world of increasingly digital telecommunications, encryption was the subject of a growing number of industrial applications. While the "cypherpunks" movement – a transnational crew of hackers keen on promoting civilian cryptography – sought to democratise its use, and while the American computer industry grew increasingly critical of export controls on crypto, law enforcement and intelligence agencies were trying to preserve their capacities to eavesdrop on telecommunications.

For a while, the NSA believed it had found the right compromise. Since 1988, the NSA had been collaborating with the National Institute of Standards and Technology (NIST), the American public standardisation body (although formally, the NIST was supposed to have escaped the NSA's supervision with the adoption of the Computer Security Act of 1987) (Burghardt, 2013). The two entities were working together on the development of a complex system that should liberalise the use of cryptography and its export while preserving the state's surveillance capabilities: the Clipper Chip. That new standard was in fact a cryptographic chip, a hardware device integrated into a telephone or a computer and equipped with an encryption algorithm – one the government said was extremely robust but was to remain classified. Each individual chip would have its own serial number and a deciphering key unique to that serial number. To eavesdrop on communications encrypted by Clipper Chips would therefore be possible only if intelligence or law enforcement agencies could get access to both the serial number and its corresponding key. Each would be stored by a different government agency, which would make them available upon judicial request and following a due process of law.

The plan was underway, but the fast-paced evolution of commercial cryptography threatened to make it irrelevant. Now, getting to convince the private sector was crucial to the whole initiative, considering that its promoters hoped to make the standard voluntary rather than compulsory. So in October 1992, when AT&T announced the roll-out of a new encryption device to be paired with telephones to secure phone calls, FBI Director William Session called AT&T's CEO to offer a deal: AT&T would use the Clipper Chip rather than its own system; in exchange, the federal government would become the number one customer for that new device and would issue reassurances about the $10 billion-plus contract then being negotiated between the telecom giant and the federal government (Levy, 2002, p. 235). The next month, Bill Clinton was elected President of the United States. Even before he took office, the intelligence community contacted his team to

convince him of the significance of the Clipper Chip. After some hesitation on the part of Vice-President Al Gore's team – which was more critical towards the demands of the computer industry – the NSA and FBI memos pointing out the dreadful consequences for "national security" of a "laissez-faire" policy in encryption seemed to leave no other alternatives for the decision-makers. After a meeting in the situation room, Clinton and Gore approved the plan.

In the U.S. hacker community, the response was immediate. Some among the cypherpunks collective proposed sabotaging the Clipper Chip or boycotting AT&T, while others contemplated enshrining the right to encryption in the constitution. Among human rights groups, the recently-created Electronic Frontier Foundation (EFF), the American Civil Liberties Union (ACLU) and others also mobilised against the government plan, creating new metaphors to make the technical developments palatable to a wide audience (for instance, they explained that the Clipper Chip was tantamount to proposing that every citizen leave the key to their house at the nearest police station). The organisation Computer Professionals for Social Responsibility (CPSR), founded in 1981, organised an online petition, circulating a letter in January 1994 from computer experts, privacy lawyers and cryptographers. In a few weeks, it was signed by more than 50,000 people, all of whom had 50,000 people, all of whom signed by sending an email to the address clipper.petition@cpsr.org with the following message: "I oppose Clipper" (Mueller, Kuerbis and Pagé, 2004). At that time, cyber-libertarians exerted a strong influence on the U.S. conservative movement, and even radio presenter Rush Limbaugh became a vocal critic of the Clipper Chip. A few months later, a CNN poll revealed that 80% of Americans were opposed to the project (Elmer-Dewitt, 2001).

The NSA tried to diffuse that opposition. Its public figure in that debate was the recently-appointed NSA General Counsel Stewart Baker. Baker would travel to a number of conferences – including the Computers, Freedom, and Privacy conference, launched in 1991 and attended by prominent hackers, EFF members and leading cryptographers. There he would face a public that was resolutely hostile to the project to try to convince them. He also made its point in the cyber-libertarian publication Wired: "Of course there are people who aren't prepared to trust the escrow agents, or the courts that issue warrants, or the officials who oversee the system, or anybody else for that matter," he wrote, denouncing a "streak of romantic high-tech anarchism that crops up throughout the computer world," Baker wrote (Baker, 1994).

But many flaws would eventually seal the fate of the Clipper Chips. For example, opponents demanded to know how criminals would be stupid enough to use a system with a built-in government backdoor, especially when end-to-end encryption tools were already available everywhere on the Internet. And since the chip was intended to be exported abroad, would global consumers really be willing to put their privacy at the mercy of the US government? A young cryptographer and political scientist, Matthew Blaze, even discovered a vulnerability allowing to circumvent the Clipper Chips' backdoor (Markoff, 1994). Meanwhile, the computer industry – under the aegis of the Business Software Alliance, the Business Software Alliance and Americans for Computer Privacy (formed by 13 companies, including Microsoft and IBM) – lobbied hard against export controls of cryptographic products and indicated that it would refuse the adoption of this new standard. That united front eventually led Congress to back their positions.

Changes in oversight: By 1996, despite modified proposals by the government, the Clipper Chip plan had become irrelevant and by then, the Department of Justice was the only significant customer for Clipper Chip-enabled devices. After months of a losing battle, in November 1996, Bill Clinton also signed an Executive Order removing encryption from the list of "weapons and ammunition" – whose export was subject to a strict regime of state authorisation – to the Commerce Control List (Al Gore would get rid of export control on strong cryptography in 2000) (Kehl, Wilson, & Bankston, 2015).

While the FBI long resisted the liberalisation of cryptography, the NSA was quicker to accept this new reality. This may have had something to do with the progress of its own cryptanalysis capabilities, other opportunities to tamper with cryptographic products. Also, in 1994 Congress passed the Communications Assistance for Law Enforcement Act (CALEA). This law forced telephone operators to include in their networks the technical possibilities for targeted surveillance of communications, even though it was not until 2004 that, on paper at least, the law was also amended to cover Internet traffic. Still, the Clipper Chip scandal, remembered as the first Crypto War, was a founding moment for the crystallisation of the discourse

of a myriad of actors in favour of civil rights against the demands of the intelligence field. Arguments based on human rights had won the day, thanks in large part to the computer industry throwing its weight in the battle.

References

Burghardt, T. (2013). The U.S. Secret State and the Internet: "Dirty Secrets" and "Crypto Wars" from "Clipper Chip" and ECHELON to PRISM. Centre for Research on Globalization. http://www.globalresearch.ca/the-u-s-secret-state-and-the-internet-dirty-secrets-and-crypto-wars-from-clipper-chip-to-prism/5357623

Kehl, D., Wilson, A., & Bankston, K. (2015). Doomed to Repeat History: Lessons from the Crypto Wars of the 1990s. New America. https://www.newamerica.org/cybersecurity-initiative/policy-papers/doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/

Levy, S. (2001). Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age. Penguin Books.

Mueller, M., Kuerbis, B., & Pagé, C. (2004). Reinventing Media Activism: Public Interest Advocacy in the Making of U.S. Communication-Information Policy, 1960-2002. Information Society, 20(3), 169–187.

Media archives

Elmer-Dewitt, P. (2001, June 24). Who Should Keep the Keys? *Time*. http://content.time.com/time/magazine/article/0,9171,164002,00.html

Markoff, J. (1993, April 16). Electronics Plan Aims to Balance Government Access With Privacy. *The New York Times*. https://www.nytimes.com/1993/04/16/us/electronics-plan-aims-to-balance-government-access-with-privacy.html

Markoff, J. (1994, June 2). Flow Discovered in Federal Plan For Wiretapping. *The New York Times*. https://www.nytimes.com/1994/06/02/us/flaw-discovered-in-federal-plan-for-wiretapping.html

UK 1996-8-1: ECHELON Gets Back in the Public Eye

In August 1996, New Zealand investigative journalist Nick Hager published his book "Secret Power" in which he detailed the "global eavesdropping network" ECHELON. This publication started a global scandal that would span over several years. Of particular outrage was the discovery that ECHELON "predominantly intercepts ordinary commercial and private communications between friendly western nations," according to a report by journalist Duncan Campbell. The system would later be the focus of debates in and reports for the European Parliament, and its existence and operation would reappear and be reaffirmed in Snowden's revelations years later.

Starting point: In August 1996, New Zealand investigative journalist Nick Hager published his book "Secret Power" in which he detailed the "global eavesdropping network" ECHELON. This global interception system was said to be the first of its kind, with its automated processing of telecommunications data through computers known as "dictionaries".The book was the first detailed account of ECHELON. Operating through the secretive UKUSA agreement, the system was initially run by both the US and the UK, and then in collaboration with the rest of what was referred to as the "Five Eyes": Canada, Australia, and New Zealand. There had been various disclosures around the ECHELON network before the release of Hager's book, although the term "ECHELON" was not named specifically or referenced under names like "P415" or "SHAMROCK".

In an interview with Ramparts magazine, Perry Fellwock (who used the pseudonym Winslow Peck) revealed the existence of this global network, without using the name ECHELON in 1972. Similarly, ECHELON was described in James Bamford's book "The Puzzle Palace" (1982) but under its previous codename "SHAMROCK", and Bamford would also later expose the NSA network "Platform"' which tied "dictionaries" (processing computers) together in the early 1990s (Hager, 1997). Shortly before Hager's publication in 1996, Duncan Campbell exposed ECHELON in a New Statesmen piece "Somebody's Listening", with the help

of information from ex-Lockheed Martin and NSA whistleblower Margaret Newsham. The dictionary system by which ECHELON operates was referenced publicly, a few years prior to the publication of Hager's book by an anonymous GCHQ source who described British interception of telex to Granada Television's World in Action in 1991, stating "And they take everything: the embassies, all the business deals, even the birthday greetings, they take everything. They feed it into the Dictionary" (Hager, 1997). Despite these previous disclosures, Hager's book provided an unprecedented level of detail about the secretive workings of ECHELON and the role of the other countries involved, with much of its information coming from sources working in intelligence agencies.

Given the past response to the Spycatcher scandal and fear of legal action by the UK and New Zealand governments, the publishers of Secret Power maintained a news blackout about their plans until the night before when copies were released in New Zealand's cities (Campbell, 1996). Even so, on the day of publication, efforts to prevent the distribution of Hager's work were discussed at "an all-day meeting of the intelligence bureaucrats in the prime minister's department" (Hager, 1997).

Wider Intelligence-related context: The scandal brought to light renewed denial in the existence of the system and the workings of intelligence agencies, as well as the extreme secrecy with which ECHELON has operated.

The foreword by David Lange, former prime minister of New Zealand, in Hager's book is one very telling example. Lange's admission of not knowing about ECHELON whilst authorising for satellites to be built revealed the levels of secrecy in which intelligence services were operating, and the absence of interests of states like New Zealand, given their (the Executive's) ignorance of systems their states were crucial to. In the case of the UK government, its continued denial and avoidance of cooperating with investigations around the ECHELON system, regardless of the numerous documentation and evidence given, was illustrated in debates in the European parliament. In one, whereby MEPs discussed American and British attitudes of refusal in cooperating, vice-chairwoman of the committee Elly Plooij-Van Gorsel stated:

> *But we must also question the behaviour of the British. When Britain held the (EU) presidency in 1997 I asked about Echelon and I was told it did not exist. Britain will have to decide where it wants to stand. How can we have a common European Union security policy if they (Britain) continue with this attitude towards other member states* (Sengupta and Castle, 2001).

Duncan Campbell (2000, p.5) expanded on the lack of protection for the privacy of international communications in his report authored for the European Parliament. He argued that the privacy of international communications was being undermined by the NSA, GCHQ, and their allies who needed these communications to be unprotected for their own interests and surveillance expansion.

Central to this scandal, and particularly seen in the frustrations of European partners, was the role of ECHELON in industrial espionage. 80 global corporations were involved in the operation of ECHELON itself, some like arms giant Lockheed Martin, playing significant roles. The global interception capabilities of agencies that had privy to commercial communications arguably prioritised US economic interests. An EU Parliament's advisory body, the Scientific and Technological Options Assessment (STOA), issued a report (1999) detailing various activities of industrial espionage in relation to ECHELON. Among these examples were US interventions against deals of Thomspon CSF and Brazil in 1994, and Airbus and the Saudi government in 1995, both of which resulted in contracts being revoked and instead given to US companies (Piodi and Mombelli, 2014, p.10).

Transnational elements: ECHELON depended on the partitioning and delegating parts of the globe to each of the Five Eyes that were part of the UKUSA SIGINT (signal intelligence) network. Parts of the world were allocated to each of the Five Eyes, with the UK responsible for Africa and Europe, east to the Ural Mountains of the former USSR. Agreements were later made with other 'Third Party' countries that became involved in the system, including, Germany, China, Japan, Turkey to mention a few examples.

Under scrutiny was the UK's role in spying on its European neighbours, whilst a member of the European Union. David Nataf, a French lawyer (who was representing French defence, aerospace, and telecommunications) articulated these concerns to the European Parliament. In one statement he pointed to

the exceptionalism of the British and the English-speaking linkage between the Five Eyes, and in another asked: “What is Great Britain, as a member of the European Union, doing participating in a programme which since the end of the Ccold war has concentrated on spying on her European partners on behalf of the United States?” (Rufford, 1998).

A crucial transnational element of the system has been the primary role of the United States. Whilst the network depends on many states, central to its operation and management is the role of the NSA, and the role of interception in relation to its interest. Although arguably its strongest partner in the management, the disparity in power is still clear in the relationship as detailed by Rufford (1998):

> *“the NSA is given a free hand to operate from Britain, supposedly ensuring that the United States shares its signals intelligence with Britain. … However, the NSA admits that although the facility is jointly operated with a minority of British personnel, GCHQ is not automatically privy to the intelligence gathered. Tapes containing data from American spy satellites are returned to NSA headquarters; the sharing of intelligence is discretionary.”*

Oversight changes: The publication of Hager’s book was followed by the adoption of oversight mechanisms beyond domestic parliaments, and particularly their usage within the European Parliament. Calls for a committee of inquiry were rejected, but a temporary committee on Echelon was set up in 2000. Numerous reports were commissioned in the late 1990s and early 2000s, and the committee heard interventions from those that contributed to these reports and STOA documents, like Nicky Hager, Duncan Campbell, and James Bamford (Piodi and Mombelli, 2014). Interventions were also provided by journalists and legal experts, and delegations were sent to Paris, London, and Washington (the latter proving to be especially hostile with intelligence agencies and authorities refusing to meet). Duncan Campbell’s ‘Signals intelligence and human rights (the ECHELON report)’ (2000) attested that there was a failure to fulfil various obligations with regards to international communications, as demanded by Article 8 of the European Convention of Human Rights, the Fourth Amendment of the US Constitution, and the Foreign Intelligence Surveillance Act.

Whilst there was clear dissatisfaction at the secretive UKUSA Agreement, trade relations meant that there was an element of caution with which European partners and the European Parliament criticised the actions of both states. This was seen for example, in the abandonment of recommendations like recommendation number 16 of the Schmid report that required the UK to explain its role in the UKUSA Alliance (Piodi and Mombelli, 2014, p.43).

The 2001 Schmid report acknowledged the existence of ECHELON and of massive industrial espionage. There was a failure in the implementation of recommendations that accompanied the report, as well as calls for more information/debate on issues like the Perkins Affair (on the role of NSA involvement in European encryption systems). The resolution and recommendations that accompanied the report and committee were limited and responsibilities were mainly outsourced to member states. The events of 9/11, only six days after the resolution was passed, saw a dismissal of these recommendations (Campbell, 2017). Another resolution was passed a year later, shedding light on the failure to act in accordance with the recommendations and calling for greater cooperation between member states intelligence services in the wake of 9/11 (Piodi and Mombelli, 2014, p.42) .

References

Hager, N. (1996a). Exposing the global surveillance system. *Covert Action Quarterly*, 11–17.

Hager, N. (1996b). *Secret Power* (Foreword by David Lange & Foreword by Jeffrey Richelson). Craig Potton.

Piodi, F., & Mombelli, I. (2014). *The ECHELON Affair: The EP and the global interception system 1998-2002* (European Parliament History Series). European Parliamentary Reserch Service (EPRS); European Parliament. https://www.europarl.europa.eu/EPRS/EPRS_STUDY_538877_AffaireEchelon-EN.pdf

Temporary Committee on the ECHELON Interception System. (2001). *REPORT on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI))*. European Parliament.

Media archives

Campbell, D. (1996). Electronic spying gleans world's 'top level secrets'. *The Independent*.

Campbell, D. (2009). *Signals Intelligence and human rights: The ECHELON report* (pp. 1–85). Electronic Privacy Information Centre. https://www.duncancampbell.org/menu/surveillance/echelon/EPIC_report.pdf

Campbell, D. (2015). My Life Unmasking British Eavesdroppers. *The Intercept*. https://theintercept.com/2015/08/03/life-unmasking-british-eavesdroppers/

Campbell, D. (2017). *Blowing the Whistle on Echelon*. https://www.youtube.com/watch?v=4l0GkE3YUpY

Campbell, D., & Lashmar, P. (2000). THE NEW COLD WAR: HOW AMERICA SPIES ON US FOR ITS OLDEST FRIEND – THE DOLLAR; EXCLUSIVE: DOCUMENTS SHED LIGHT ON US POLICY OF COVERT SURVEILLANCE OF BRITISH AND EUROPEAN INDUSTRY. *The Independent*.

Rufford, N. (1998). Spy station F83. *The Sunday Times*.

Sengupta, K., & Castle, S. (2001). SECRECY, SPY SATELLITES AND A CONSPIRACY OF SILENCE: THE DISTURBING TRUTH ABOUT ECHELON. *The Independent*.

U.S. Electronic Espionage: A Memoir. (1972). *Ramparts*, *11*(2), 35–50.

US 2000-6-1: A Tepid ECHELON Controversy

The *ECHELON scandal had much less coverage in the US, especially relative to the US's role in the network. Like the UK, much of the controversy and debate about the global signals intelligence network arose after the involvement and publications of the European Parliament, that came in the wake of the publication of Nicky Hager's book (although ECHELON had been uncovered decades before). According to Balint (1999), much of the conversation around ECHELON in the US was prompted by investigative foreign journalists. The scandal saw tensions between intelligence bodies and lawmakers, as well as unlikely alliances formed in its wake, demanding more information and oversight, and raising public awareness about the network.*

Starting point: The network, run by the Five Eyes, had itself come about before the 1950s from the UKUSA agreement that followed previous Signal Intelligence (SigInt) collaborations, such as the 1943 Britain USA agreement (BRUSA) and in spaces like the Commonwealth Signal Intelligence Conference (1946-47). Communications are transmitted through satellite, radio, and a "combination of water cables under oceans and microwave networks over the land" (Hager, 1996, p.14) before chosen keywords are used to filter these communications at "Dictionary" computers of ECHELON stations (ibid).

Like the UK case, much of the attention with regards to the ECHELON scandal came after the involvement of the European Parliament in the mid-late 1990s and early 2000s, although much about ECHELON had been uncovered previously by journalists and whistle-blowers. Important in the revelations of ECHELON was its reference in NSA responses to Freedom of Information requests in the 1990s conducted by Dr. Jeffrey Richelson at the National Security Archive, George Washington University (Agence France Presse 2000; Zeller 2000; Richelson 2005).

Wider intelligence conversations: There were various elements to the scandal that spoke to wider concerns/practices around intelligence. Outlined here are issues of economic espionage, encryption, and surveillance on campaigning/resisting actors. Attention and criticism of the US, and the NSA more specifically, came with regards to the reports of economic espionage. The use of signals intelligence to advantage US economic interests were made explicit in a 2004 interview in *Slate* magazine, where the director of the NSA from 1977-1981 Bobby Ray Inman spoke to the transnational and primarily economic-driven operation of ECHELON: "It wasn't just Europe; it was worldwide" … "Its real impact was economic, on financial issues" (Keefe, 2006, p.246).

It is worth noting the focus on economic intelligence under Clinton's administration which oversaw the setting up of the National Economic Council (NEC) that worked closely with the NSA and CIA for US

commercial advantage (Ford, 1999). Perhaps ironic is that the US was at the same time targeting "foreign industrial spies" and trying to clamp down on economic espionage. One example of this is Clinton's signing of the 1996 Economic Espionage Act – which at the time was considered to be "the first nationwide US statute prohibiting the theft of trade secrets" that saw convictions and collaborations with the Justice Department (Ford, 1999). Attempts at limiting encryption from the US government were being undermined with the exposure of the ECHELON network (ibid). The persuasion of European governments to provide the US with hidden keys and exemptions to encryption became less favourable given the disclosures of economic espionage that left them in less favourable economic situations than their US counterparts.

Linked to the preservation of US economic interests, but much less reported on, was the role of ECHELON in gathering intelligence on groups like Amnesty International, Christian Aid, and Greenpeace (Blumner, 1999). High profile cases like the gathering of information on Princess Diana, who had supported campaigns against landmines, received more attention with the NSA being forced to release over 1000 pages they'd gathered on her (Temporary Committee on the ECHELON Interception System, 2001). Intelligence gathering on activities, groups, and people that were at odds with or threatened US foreign (/economic) interests cannot be understated and expose the more visible and far-reaching effects of intelligence.

Another area that received less attention comparatively was the concerns around infringements on rights and privacy. However, this topic did bring about vocal dissidence within Congress and civil liberties organisations.

Transnational elements: The network is transnational by its extensive operational nature that covers the globe, and thereby in the effects that this transnational network has in directing foreign (and/ economic) policy and prioritising specific interests.

In 1998, the *Associated Press International* reported the coverage from a major newspaper in Tokyo uncovering the European Parliament's response to the scandal, and the economic espionage involved. This included the role of the CIA and British Intelligence. Amongst other similar examples of economic espionage (e.g. with French company Thomson-CSF), the article detailed the NSA's involvement in pressuring Jakarta to award half a contract to the American conglomerate AT&T after "1990 negotiations between Japan's NEC Corp and the Indonesian government over purchase of telecommunications machinery" (Associated Press, 1998). *St. Petersburg Times* (Florida) in 1999 reported that a former NSA employee had exposed American spying on the German energy company, Enercon (Blumner, 1999). Many more examples like these have been exposed, and a few of these are discussed in the UK overview.

Central to the operation of the network, was the transnational collaboration of signals interception, primarily amongst the Five Eyes. It has been suggested that this transnational arrangement is necessary to avoid responsibilities and avoid oversight mechanisms (e.g. by depending on partners to provide intelligence on domestic populations). This has been elaborated on by ex-CSE officer Mike Frost (Klein, 2000), and by Keefe (2006). Although the US depended heavily on other 'eyes' for signals intelligence, it should be noted that power dynamics amongst SigInt partners varied, even for the most established partners like the UK. The UK would only have access to information after the US had overseen it:

One former NSA officer put it thus: "[All] information comes to the United States, but the United States does not totally reciprocate in passing information to the other powers." Indeed, most of the American bases located on foreign soil, including RAF Menwith Hill, send intelligence directly back to Fort Meade, Maryland, after which it can be distributed to other powers on a need-to-know basis. Though Britain houses the giant ear at Menwith Hill, it hears only what America wants it to (Keefe, 2006, p.20).

Much of the transnational focus and attention was based on the role of ECHELON in economic and trade relations that Hager and the European Parliament exposed and expanded on. The monitoring of states in the General Agreement on Tariffs and Trade (GATT) provided by Hager in his book (1996) is one example of how ECHELON gave the US the upper hand with trade negotiations (Blumner, 1999).

Changes in oversight: This heavier focus on the transnational role of ECHELON also brought about a transnational element to exercising and testing oversight. This is evident in examples documented in the overview of the US case, as well as cases such as a Swedish government investigation and Italian inquiry

into the NSA's possible breach of privacy law (Ford, 1999), and efforts of the French government to sue both UK and US governments also on grounds of privacy breaches (Gold, 2000).

Within the US, an understanding of the lack of judicial and legislative oversight has to take into consideration the denial and refusal to engage with the scandal (and the existence of the network itself), a tactic also adopted in the UK. The European Parliament reports were largely dismissed, regardless of their return to the spotlight with significant events like 9/11 and the Snowden revelations. Perhaps a telling case of (an absence of) oversight is the case of Margaret Newsham whose concerns about breaches of constitutional law and privacy were not addressed when raised, whilst she worked *within* the NSA. Tensions on matters of oversight were seen between the NSA and lawmakers when the NSA refused 'the Permanent Select Committee on Intelligence's request for internal legal memoranda and documents produced by the agency's general counsel', asserting "attorney-client privilege" (Dupont, 1999, p.2). Similarly, in April 2000, the head of the NSA, and director of the CIA testified at the US House Intelligence Committee denying "reports the United States was involved in spying on Europeans and Americans as part of a satellite surveillance network" (Brand, 2000). This refusal to admit and engage was adopted as strategy on the global scale - and bodies like the European Parliament temporary committee on Echelon had limited remit, access, and oversight power. The Bush Administration, NSA, and CIA all refused meetings with this temporary committee upon their delegation to Washington in the early 2000s (Meller, 2001). Requests for information through the FOIA about ECHELON were often delayed and denied.

However, pushbacks did exist in different forms, including through the Houses of Representatives. In May 1999, Bob Barr, in his concerns around (lack of) legal mechanisms and privacy protection, amended the Intelligence Reauthorization Act, requiring "the Attorney General, and the directors of the National Security Agency and the Central Intelligence Agency to provide a detailed report to Congress, explaining the legal standards the intelligence community uses to monitor the conversations, transmissions, or activities of American citizens" lack (Congressional Press Releases, 1999). Porter Goss, the chairman of the House Select Committee on Intelligence, who had raised concerns regarding the breadth of permissions for intelligence gathering and interpretation, had failed to retrieve documents from the NSA about the reach of Echelon (MacMillan, 1999). In the face of this, the Electronic Privacy Information Center (EPIC) filed a lawsuit demanding the release of these documents (ibid). As mentioned above, this concern for privacy rights saw unlikely collaborations between groups like the ACLU and conservative congressmen like Barr. ACLU also joined Electronic Privacy Information Center (EPIC) in the US to form groups like Echelon Watch in order to raise public awareness (Krebs, 1999). The European Parliament reports urged citizens and businesses in Europe to use and develop open-source encryption (Verton, 2001). Other less formal pushbacks included a day of action - "Jam Echelon Day" - organised by hacktivists on the 21st October 1999, in an attempt to jam the network (Balint, 1999). Although considered to be a too ambitious aim, experts agreed that it raised awareness.

It is worth noting that even critical voices on the (lack of) transparency or oversight have adopted a language of necessary intelligence along racialised and securitised lines. This can be seen especially amongst dissidents within intelligence agencies, like Margaret Newsham's concerns that were raised when she heard "American voices" (Klein, 1999), or Canadian whistleblower Mike Frost's concerns that were primarily focused on the domestic realm of eavesdropping (ibid).

References

Hager, N. (1996). Exposing the Global Surveillance System. *Covert Action Quarterly*, *59*, 11–17.

Keefe, P. R. (2006). *Chatter: Uncovering the echelon surveillance network and the secret world of global eavesdropping*. Random House Trade Paperbacks.

Meller, P. (2001, May 11). European Parliament snubbed by United States over Echelon. *InfoWorld Daily News*.

Richelson, J. (2005). *The National Security Agency: Declassified*. https://nsarchive2.gwu.edu/NSAEBB/NSAEBB24/index.htm#docs

Temporary Committee on the ECHELON Interception System. (2001). *REPORT on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI))*. European Parliament.

Media archives

Balint, K. (1999, October 17). Spy in the sky? That could be Echelon. *Copley News Service*.

Blumner, R. E. (1999, April 18). Echelon listens around the world. *St. Petersburg Times*, 1.

Brand, C. (2000, September 12). EU echelon probe set to ask top US officials to testify. *The Associated Press*.

Declassified documents confirm secret worldwide US surveillance network. (2000, February 4). *Agence France Presse*.

Dupont, D. G. (1999). NSA'S 'ECHELON' PROGRAM TO COME UNDER SCRUTINY IN HOUSE HEARINGS. *Inside the Pentagon*, *15*(34), 2–2. JSTOR.

Echelon. (2000). Columbia Broadcasting System; Academic Video Online: Premium database. https://search.alexanderstreet.com/view/work/bibliographic_entity%7Cvideo_work%7C2780993

Ford, P. (1999, September 3). Friction over 'friendly' spying. *The Christian Science Monitor/The Monitor*, 1.

Gold, S. (2000, February 11). French Govt Could Sue US & UK Over Echelon Spy Network. *Newsbytes*.

Krebs, B. (1999, December 13). NSA Reveals Echelon Spy Net Info To Congressman. *Newsbytes*.

MacMillan, N. (1999, December 3). Privacy Group Sues NSA For Echelon Disclosure. *Newsbytes*.

Spy agency helped U.S. companies by listening in on competitors: Report. (1998, September 19). *Associated Press International*.

TARGET OF BARR AMENDMENT. (1999, May 13). *Congressional Press Releases*.

Verton, D. (2001, June 4). Report Warns Europeans About Echelon Surveillance; Urges firms, citizens to use encryption. *Computerworld*, 20.

Zeller, T. (2000, July 16). Ideas & Trends; Cloak, Dagger, Echelon. *The New York Times*, 16.

UK 2003-03-02: Blowing the Whistle on GCHQ's Surveillance of UN Diplomats

On the 2nd of March 2003, The Observer published a front-page headline "Revealed: US dirty tricks to win vote on Iraq". The piece detailed a leaked memo from the US National Security Agency (NSA) to GCHQ that asked for support in spying on UN Security members in order to influence voting intentions on the Iraq war. The email had been leaked by GCHQ translator, Katharine Gun, who had received the email from Frank Koza at the NSA at the end of January 2003. Gun printed and leaked the document, in the firm belief that the public should know of the illegal means in which the war on Iraq was being pushed. Gun was charged with breaching the Official Secrets Act in 2004, but her case was swiftly dropped within a few hours, after her defence demanded the disclosure of the Attorney General's legal advice for going to war.

Starting point: On the 31st of January 2003, Katharine Gun who was working as a translator at GCHQ, received an email from the "Head of Regional Targets at the National Security Agency (NSA), Frank Koza. The email had asked for UK help with "a surge" concerned with intensifying intelligence-gathering operations of UN members. Koza (2003) was after "the whole gamut of information that could give US policymakers an edge in obtaining results favorable to US goals or to head off surprises. In RT, that means a QRC surge effort to revive/ create efforts against UNSC members Angola, Cameroon, Chile, Bulgaria and Guinea, as well as extra focus on Pakistan UN matters." Upon the shock and anger Gun had experienced when reading the email, she decided to print and leak the memo to a friend who passed it onto the press. A few weeks later, on the 2nd of March 2003, Gun saw *The Observer*'s front-page detailing contents of the memo she had leaked.

Wider intelligence-related context: The leaked memo was accompanied by other revelations of spying on the United Nations at the time, raising further questions about the legality of the war, and the efforts of both the US and UK in pushing for an invasion. Ex-former member of the Cabinet and British International Development Secretary, Clare Short, who had resigned 8 weeks prior to the war, also contributed to the conversation on UN snooping. In an interview about Katharine Gun's case on the *BBC*'s Today Programme, on the 26th of February 2004, Short declared that the UK was spying on Kofi Annan's office, and that "these things are done and in the case of Kofi's office it's been done for some time" (Short, 2004). These statements complimented Chile and Mexico's complaints to the UK with regards to being spied on (Bright et al., 2004). Whilst the spying on various officials was being publicly discussed, for Gun, the *manipulation* of intelligence was crucial to this scandal, as recounted in Keefe (2006, p46): "It wasn't just the fact that they were listening, it was what they were going to do with the information," Katharine said. "It was because it was about the issue of war, the issue of human lives, the issue of the workings of the UN and manipulating it in such a way as to secure the result of war."

Gun had been charged under the Official Secrets Act. The Official Secrets Act is "national security" legislation aimed at preventing the disclosure of state secrets and government information. The Act (used in the UK and many former British colonies) was originally passed in 1911 but has since been reviewed in 1989. There have been attempts at removing/reforming (parts of) the Act, and other calls for it to be replaced with another Act (e.g an Espionage Act) to expand its scope and powers further. The case of Katharine Gun saw the defence of necessity being adopted successfully for the first time. The defence had been rejected for a previous breach of the Official Secrets Act by former MI5 officer David Shayler, who disclosed information on MI5 intelligence on Labour ministers, information relating to the IRA bombing of Bishopgate in 1993, the bombing of the Israeli embassy in 1994, and MI6 involvement in a plot to assassinate Muammar Gadafy (Norton-Taylor, 2001).

Although the Attorney-General, Lord Goldsmith's (2004) claim that Gun's case was "a clear prima facie breach of Section 1 of the Official Secrets Act 1989", he affirmed the defence of necessity was used to abandon the trial, and that it was based on "solely legal grounds … and free from any political interference". The swiftness in which the defence of necessity was adopted has been questioned, particularly because of the defence's demands for disclosure of the full legal advice provided by Goldsmith in favour of the war. The former defence secretary under Tony Blair, Geoff Hoon, later recounted how he was ordered to burn the memo on the legality of the war from the Attorney-General (Elgot, 2022). The successful adoption of the defence of necessity also drew conversation to "acceptable" and legal means of breaching the Official Secrets Act.

Transnational dimension: There are many transnational elements to this scandal. First and foremost, this case was concerned with the invasion of Iraq, and therefore Iraqis are central to it. The collaboration of GCHQ and NSA in UN spying operations shed light on other transnational elements of this case. The specific attempts of intensifying spying on, and influencing voting intention, particularly of newer members of the UN Security Council, indicate(d) the power imbalances present in "international" bodies. Koza's call for help "to give the United States 'the edge' in the crucial forthcoming negotiations over authorising war in Iraq" (Bright et al. 2004) reveal not only transnational alliances, but the undermining of supposedly internationally democratic institutions.

Katharine Gun's case of course presented transnational elements in solidarity as well, being cited in calls for whistleblowers to be courageous, and take example from her. Her case drew support from whistleblowers across the world, famously including Daniel Ellsberg, responsible for the Pentagon Papers leak in 1971. Ellsberg had praised Gun stating that her leak was "the most important and courageous leak I have ever seen. No one else – including myself – has ever done what Gun did: tell secret truths at personal risk, before an imminent war, in time, possibly, to avert it" (Adams, 2019).

Change in oversight: Katharine Gun's case saw with it calls for the reform of the Official Secrets Act. This included small calls, such as those from her family [her mother expressed the wish for "some permanent long-term good" and exclaimed her disapproval at the treatment of whistleblowers (Bright, 2004)]. Parliament saw a number of questions and debates about lines of defence that would be acceptable in the

breach of the Official Secrets Act. An early day motion: EDM 691 was tabled on the 25th of February 2004, and signed by 30 signatories. The EDM (2004) praised Gun and called on the government to amend the Official Secrets Act, allowing for a public interest defence that would protect whistleblowers like Gun, as well as asking for a statement from the government on the information exposed by Gun.

Perhaps more significant was the collaboration of whistleblowers and oversight efforts outside of Westminster. Gun's case had seen whistleblowers come together in a symposium, including "former FBI employees Coleen Rowley and Sibel Edmonds, Major Frank Grevil from the Danish intelligence community and others who have spoken out about the abuses, cover-ups and lies that our respective governments have peddled before and after the invasion of Iraq" (Gun, 2004). A later formation of a Truth-Telling Coalition saw global partners call for efforts from whistleblowers, and for their support and protection. In the UK, this consisted of calling for reforms on the Official Secrets Act. Significant also, is the role of organisations like Liberty who had represented Gun and demanded disclosure of the legal advice provided for war, as well as protecting a whistleblower.

To a certain extent, however, it can be argued that little changed, especially relative to what the leak intended to do. Gun has expressed her disappointment in the lack of accountability and action that followed, describing a common "blasé attitude – the spying goes on, everyone does it and so it's nothing to get all hot under the collar about" (Bright, 2013), whilst acknowledging the leak's significance in exposing this "ugly truth". Both journalists Martin Bright and Ed Vulliamy (2019) who helped publish the story in *The Observer* in 2003 have described their disappointment in the failed attempt of the leak at doing more to stop the war. However, given its relatively recent history, and the related calls of disclosure that have still not been answered, the effects of the scandal are still present and both Bright and Vullimay (2019) urge for the power of this scandal to fulfil its potential.

References

Katharine Gun. (2004). Hansard. https://hansard.parliament.uk/Lords/2004-03-10/debates/ded1e4ef-b4fd-4cac-8f94-e5bc2dd42e58/KatharineGun?highlight=katharine%20gun#contribution-1034d9ee-68a5-4352-9b51-5f6794f24553

Katharine Gun and Reform of the Official Secret Act, n°. EDM 691 (2004). https://edm.parliament.uk/early-day-motion/25426/katharine-gun-and-reform-of-the-official-secrets-act#tab-supporters

Keefe, P. R. (2006). *Chatter: Uncovering the Echelon surveillance network and the secret world of global eavesdropping*. Random House Trade Paperbacks.

Media archives

Bright, M. (2004, February 22). GCHQ mother: My girl is not a traitor. *The Guardian*. https://www.theguardian.com/politics/2004/feb/22/iraq.freedomofinformation

Bright, M. (2013). Katharine Gun: Ten years on what happened to the woman who revealed dirty tricks on the UN Iraq war vote? *The Guardian*. https://www.theguardian.com/world/2013/mar/03/katharine-gun-iraq-war-whistleblower

Bright, M., Vulliamy, E., & Beaumont, P. (2003). *Revealed: US dirty tricks to win vote on Iraq war*. https://www.theguardian.com/world/2003/mar/02/usa.iraq

Democracy Now! (2019, July 19). *15 Years Later: How U.K. Whistleblower Katharine Gun Risked Everything to Leak Damning Iraq War Memo*. https://youtu.be/CWtIu7mbnbM

Elgot, J. (2022, January 5). Geoff Hoon 'told to burn memo that said Iraq invasion could be illegal'. *The Guardian*. https://www.theguardian.com/politics/2022/jan/05/geoff-hoon-told-to-burn-memo-that-said-iraq-invasion-could-be

Gun, K. (2004, September 19). Comment: The truth must out: Katharine Gun faced jail for revealing US plans to bug UN delegates in the run-up to the war on Iraq. Now the ex-GCHQ worker insists we should cherish our whistleblowers, not punish them. *The Observer*, 31. ProQuest One Academic.

Katharine, G. (2019, September 22). *Interview: Iraq war whistleblower Katharine Gun: 'Truth always matters'* (T. Adams, Interviewer) [Interview]. https://www.theguardian.com/film/2019/sep/22/katharine-gun-whistleblower-iraq-official-secrets-film-keira-knightley

Martin, B., Hinsliff, G., Barnett, A., Harris, P., Tuckman, J., & Vulliamy, E. (2004, February 29). Focus: The UN spy scandal: SPECIAL REPORT: WHISTLEBLOWER: For the first time, The Observer can reveal the full story behind Katharine Guns revelations about spying at the UN which have plunged the Government into crisis. *The Observer*, 17. ProQuest One Academic.

Norton-Taylor, R. (2001, September 29). Blanket ban of secrets act ruled unlawful. *The Guardian*. https://www.theguardian.com/uk/2001/sep/29/freedomofinformation.Whitehall?CMP=gu_com

Sherwood, B., & Tait, N. (2004). Secrets law to be reviewed in wake of Gun case. *Financial Times*.

Transcript of Clare Short interview. (n.d.). http://news.bbc.co.uk/1/hi/uk_politics/3489372.stm; http://news.bbc.co.uk/media/audio/39859000/rm/_39859206_spying08_short26_long.ram

US plan to bug Security Council: The text. (2003). https://www.theguardian.com/world/2003/mar/02/iraq.unitednations1

DE 2005-11-10: The BND Spies on Journalists

The Bundesnachrichtendienst (BND) tapped into the telephone lines of numerous journalists to expose possible secret service employees who would have passed on insider knowledge between 1993 and 1998. This illegal surveillance of German journalists was conducted by an element within the BND named "QC 30" that was initially supposed to monitor BND-employee activities. It went on for many years without informing the head of department. QC 30 worked like a secret service within the secret service, "out of control and thus outside the law" as one newspaper put it. By the time of the scandal, responsible figures had already been dismissed and except for a parliamentary inquiry, no significant consequences ensued.

Starting point: In 2005, after conducting his own investigation, intelligence scholar and journalist Erich Schmidt-Eenboom published evidence proving that the BND has been surveilling him from 1993 up until 2003. Crucially, the (illegal) operation was only approved for the period between 1993 to 1996. The surveillance beyond that date was acknowledged by the head of BND August Hanning and Ernst Urhlau, Intelligence Coordinator at the Federal Chancellery, the German Seat of Government in 2005. Hanning said at a press conference: "I cannot exclude the possibility that disloyal employees were under surveillance, and I cannot exclude the possibility that journalists came into view in the process".

Literature suggests that two parallel occurrences led the BND to surveil journalists in Germany. The first was the publication of Erich Schmidt-Eenboom's book "*Der BND: Schnüffler ohne Nase – die unheimliche Macht im Staate*" in 1993 which contained insider knowledge. The second was a *Spiegel* article that uncovered the so-called plutonium scandal. It exposed a BND operation in which plutonium was smuggled from Moscow to Munich in a civilian aeroplane in 1994. The BND began to investigate who could have passed the classified information to the journalist. Within this context, they started to systematically and illegally surveil German journalists and even recruited journalists as assets to get information on their colleagues from 1993 up until 1998. Among others, Schmidt-Eenboom was also surveilled by the BND in 1995 and 1996 due to his activity in publishing books about intelligence services. However, contrary to the claims of the BND, the surveillance went up until 2003, as he collected evidence that the content of his office's trash can was seized covertly. This surveillance was conducted by a group within the BND named "QC 30". This was lastly acknowledged in 2005 by BND Chief Hanning after Schmidt-Eenboom requested disclosure on his surveillance from the BND while bringing forward evidence.

Wider intelligence-related context: The scandal focused on three key issues: the illegal surveillance of domestic journalists, the recruitment of domestic journalists in order to find information on potential moles, and the evasion of internal scrutiny and oversight by the QC30. According to the parliamentary inquiry report, the then head of the BND, Konrad Porzner, admitted having authorised the initial surveillance of Schmidt-

Eenboom, but claimed to not have authorised further surveillance from 1996 onwards. This stands in contrast with the surveillance evidence Schmidt-Eenboom found. In turn, it indicated that the practices of the BND operatives' diverged from the orders of the higher-ups. The inquiry was also connected to other practices in which the BND was involved and that led to Bundestag inquiries. These included the BND role in providing transport to so-called CIA black sites (in particular Guantanamo Bay) done by routing flights via Germany; the provision of information to foreign agencies that contributed to the abduction of Khaled el-Masr, a German national who was associated with an islamist millitant group in his youth, as well as BND agents giving critical information to U.S. intelligence agencies in Baghdad; outside of the chain of command.

Change in oversight: Besides the inquiry committee of the 16th Bundestag, there were no apparent consequences with regard to oversight. The final report generally viewed parts of the observation operation as illegal but no policy-changes followed. Responsibility for the illegal practices seeped away due to numerous personnel changes at the top level of the BND between 1993 when the scrutinised practices started, and 2005 when the affair became public. Bernd Schmidbauer, who was the Intelligence Coordinator at the Federal Chancellery at the time of the surveillance measures, declared in 2006 that he would suspend his work as a member of the Parliamentary Oversight Body (PKGR) until further clarification.

Media archives

Krischer, M., Spilcker A. (2013, November 13). BND-SKANDAL: QC 30 außer Kontrolle. *Focus.* https://www.focus.de/politik/deutschland/bnd-skandal-qc-30-ausser-kontrolle_aid_208870.html

Niebel, I. (2007, December 17). Eine unendliche Skandalgeschichte – Die "Embedded Journalists" der Geheimdienste. *Bürgerrechte und Polizei.* https://www.cilip.de/2007/12/17/eine-unendliche-skandalgeschichte-die-embedded-journalists-der-geheimdienste/#_ftn4

Die Hand im Feuer (1995, April 23). *Der Spiegel.* https://www.spiegel.de/politik/die-hand-im-feuer-a-64ba53fd-0002-0001-0000-000009180723?context=issue

German Intelligence Agency Spied on Journalists. (2005, November 10). Dw.Com. https://www.dw.com/en/german-intelligence-agency-spied-on-journalists/a-1772654

References

Schäfer, Gerhard (2006, May 26). *Report of the expert commissioned by the parliamentary control body of the German Bundestag*. Deutscher Bundestag. http://webarchiv.bundestag.de/archive/2010/0304/bundestag/ausschuesse/gremien/pkg/bnd_bericht.pdf

Foertsch (2009, February 12). *Journalistenkontakte sollten BND-Lecks aufdecken.* Deutscher Bundestag. https://web.archive.org/web/20090719072327/http://www.bundestag.de/aktuell/hib/2009/2009_047/01.html

Final report of the Inquiry Committee of the 16th Bundestag, printing matter 16/13400 (2009). https://dip21.bundestag.de/dip21/btd/16/134/1613400.pdf

Schmidt-Eenboom, Erich (1993). *Schnüffler ohne Nase: Der BND – die unheimliche Macht im Staate.* Düsseldorf, Wien, New York, Moskau: ECON-Verl.

US 2006-6-13 Mark Klein Blowing the Whistle on NSA/AT&T Surveillance

The 2006 AT&T scandal brought to the fore new evidence about NSA-private sector warrantless surveillance. Mark Klein, an employee of the company AT&T, discovered a splitter that duplicated every communication of AT&T customers that was then provided to the NSA. After an Electronic Frontier Foundation lawsuit, the US Congress passed the FISA Amendments Act in July 2008, which retroactively provided immunity to the companies cooperating with the NSA, whilst also further removing legal protections for foreigners.

Starting point: In 2006, the Electronic Frontier Foundation (EFF) filed a class lawsuit against AT&T for submitting terabytes of customer communications without a warrant. Shortly after, USA Today ran a story detailing the extent of the programme. Three years prior, in 2003, Mark Klein, an AT&T communication technician, discovered that the NSA was tapping the company - a practice that he discovered stretched back to 1985. Klein discovered *Room 641A*, a restricted space with no door handle and cables that went upstairs to the room where AT&T handled internet connections. Curious about the cables, he found that the information processed in Room 641A went to a "splitter": delivering information to the room of AT&T's connections, as well as its known destination. This allowed AT&T to make duplicates of every fibre signal. On 13 April 2006, EFF's litigation led to an article in the New York Times based on Klein's documents (Markoff & Shane, 2006).

Wider intelligence-related context: This scandal came to light shortly after the 2005 warrantless surveillance program was revealed by the New York Times scandal. Klein's discovery, and the documents he gathered demonstrating that the "peering connections" from AT&T and other networks were indiscriminately intercepted, offered specific evidence of how these programs ran. The splitter, Klein was sure, allowed for bulk surveillance as it had no selective capabilities; - it just copied all international and domestic traffic. To put this in numbers, "by 2013 the program was processing 60 million foreign-to-foreign emails a day" (Angwin, 2015). Later information demonstrated that AT&T also "provided technical assistance in carrying out a secret court order permitting the wiretapping of all Internet communications at the United Nations headquarters, a customer of AT&T" (Angwin et al, 2015). In addition, it was reported that there were more AT&T facilities such as Atlanta, and probably San Jose, Los Angeles, San Diego and Seattle (Markoff & Shane, 2006). At first, Klein hesitated about going public, knowing he would be discredited by his company and by the NSA. However, in 2006, Klein came forward with the support of the Internet Frontier Foundation. The NSA initially argued that it was foreign-foreign communication interception, but the EFF helped Klein demonstrate the domestic dimension.

Change in oversight: The US Government attempted to block the process using state secrets privilege, which was rejected by the courts. Before a decision on a subsequent appeal by the US Government was delivered, Congress passed the FISA Amendments Act in July 2008. While it was nominally concerned with 'better' oversight (e.g., requiring to complete an annual comprehensive review by the Inspectors General of all agencies), it also extended the capabilities of interception by intelligence agencies.

Most notably, The Act provided a retroactive immunity to companies participating in wiretapping programs with the government of the United States, bringing to a close the lawsuit against AT&T. This decision was described by Senators like Chris Dodd as contrary to the rule of law. Additionally, the 2008 FISA Amendment Act added Title VII, which essentially removed any protection of foreigners located outside the United States. This amendment renovated *de facto* many of the measures introduced by the Patriot Act, which had expired that year.

However, crucial to note, is that this case was also important for the vitality of anti-surveillance movements, as it brought to light documents that demonstrated the scope of both the capabilities and cooperation between the agencies and the private sector (Markoff & Shane, 2006).

References

Klein, M., & Bamford, J. (2009). *Wiring Up the Big Brother Machine--and Fighting it*. BookSurge.

Media archives

ACLU. HEPTING V. AT&T: CHALLENGING CORPORATE COLLUSION WITH THE NSA. https://www.aclu.org/other/hepting-v-att-challenging-corporate-collusion-nsa

Angwin, J., Savage, C., Larson, J., Moltke, H., Poitras, L., & Risen, J. (2015). AT&T helped US spy on Internet on a vast scale. *The New York Times*, *15*.

Poulsen, K. (2007) Mark Klein Documents (Wired) https://www.wired.com/images_blogs/photos/uncategorized/2007/05/09/2_3.jpg

Martin, A. (2009) . Review of Klein's Wiring Up The Big Brother Machine… And Fighting It. Surveillance & Society 6(4): 416-417. http://www.surveillance-and-society.org

Markoff, J., & Shane, S. (2006). Documents Show Link Between AT&T and Agency in Eavesdropping Case. *New York Times*, *13*, A1.

Markoff, J (2006). U.S. Steps Into Wiretap Suit Against AT&T. *New York Times.* https://www.nytimes.com/2006/04/29/us/us-steps-into-wiretap-suit-against-att.html

FR 2008-07-01: The EDVIGE scandal

In June 2008, the French government merged the two main domestic intelligence agencies, and in the process expanded a database dedicated to the general surveillance of French political life. Brought to the fore of public attention, the database – named EDVIGE – unleashed a widespread civil society opposition, leading the government to backtrack and put the broader plans for modernising intelligence law to rest until the end of its mandate. But once the controversy lapsed, the sort of data that EDVIGE aimed at collecting was included in a new database. Although the latter came with important restrictions compared to the original plan, these would soon be lifted. Meanwhile, lacking the sort of public pressure that had proven key in 2008, the demands of institutional oversight actors to play a greater role in supervising intelligence and police databases have fallen on deaf ears.

Starting point: On the 1st of July of 2008, the French government officially published an executive decree merging two distinct domestic intelligence agencies – DST (*Direction de la surveillance du territoire*) and part of the RG (*Renseignements généraux*) into the *Direction centrale du renseignement intérieur* (DCRI). That same decree also reorganised the existing databases used by DST and RG. As part of the merger, part of the RG database dedicated to general political surveillance – which for the most part only indexed information archived on paper in various regional offices of the RG – would now be called by the acronym EDVIGE (Mafart, 2018). It gathered data on three categories of people or organisations: elected officials and political parties, trade unions, religious or business leaders as well as activists; people deemed a likely threat to public order; people seeking a position in public administrations and subject to an administrative inquiry.

The 2008 decree made clear what had hitherto remained tacit in the legal framework: that domestic intelligence was sometimes concerned with mainstream, non-criminal political activity, and that in the process of this surveillance, sensitive data, e.g. related to health or sexual orientation was being gathered. As Le Monde's article (which was published on the same day) made clear, the new database "will contain all the information collected in the context of the so-called 'open intelligence' and (…) will authorise the registration of minors from the age of 13 if they are considered 'likely to be a threat to public order'" (Le Monde, 2008).

Intelligence-related context: One year into the presidential mandate of Nicolas Sarkozy, the creation of EDVIGE stirred fears of a Big Brother government, all the more considering that since a 2004 reform, the ex ante opinions on government surveillance programs issued by the CNIL, the French data protection agency, had become non-binding. In the specific instance that lead to the creation of EDVIGE, the CNIL had asked that minors under sixteen be kept out of the database, that the collection of sensitive data (e.g. on ethnic origins, health status, or sexual life) be more strictly circumscribed, and to establish a time limit on data retention. It had also asked that the database be created by a legislative act rather than a decree, to allow for a parliamentary debate to take place. But the government chose to disregard most of these suggestions and went ahead with its initial plan (Chemin, 2008).

Within 10 days of the decree's publication, several non-profit organisations – composed for the most part of trade unions and humans rights organisations – joined forces to launch an online petition under the banner "*Non à EDVIGE*." In just a few weeks, the petition, which claimed that EDVIGE was conducive to a "level of surveillance of citizens totally disproportionate and incompatible with the concept of the rule of law", gathered more than 220,000 individual signatures as well as the support of 1,200 organisations. LGBTQ+ organisations, HIV and AIDS nonprofits, youth and environmental groups, and disability rights groups

expressed massive support for the petition (Marzouki, 2009). Elected officials and political parties also came out strongly against EDVIGE. Several legal challenges – including one by the "Non à EDVIGE" coalition – were introduced before the Council of State, alleging that the decree was illegal and violated international human rights law. The United Nations Committee on Human Rights also stressed that EDVIGE contradicted the International Pact on Civil and Political Rights (Piquemal, 2009).

Oversight changes: The scandal was big enough for the government to backtrack. In September 2008, the Interior minister, Michèle Alliot Marie, announced that a new decree would be adopted so health data and information on people's sexual orientation would be struck down, and that minors would be granted a "right to be forgotten", where data would be deleted after five years if they are no longer deemed a "threat to public order".

Meanwhile, at the National Assembly, a parliamentary working group was put together to draft a report on law enforcement and intelligence databases. The original intent was to pave the way to a legislative framework – this was the essence of the 9 recommendations put forward in March 2009, of a proposed bill and of the committee report eventually published more that three years later (Batho & Béinisti, 2011). However, it was never to be the case. If anything, the EDVIGE scandal stood as the confirmation of the widely-held belief that, in these matters, those in charge of political surveillance are best advised to minimise publicity. This was to the extent that, whereas in July 2008 the government had released a White Paper of Defense and National Security calling for detailed intelligence legislation, the mobilisation against EDVIGE was apparently enough to put the government's broader plans for modernising intelligence law to rest until the end of its mandate. The reform only took place in 2015 under a left-wing government (Tréguer, 2017).

As for EDVIGE's successor, the government chose not to go to parliament to seek legislative backing. Instead, it adopted a new decree– nicknamed EDVIGE 2 but whose official name is "*Prévention des atteintes à la sécurité publique*" (PASP). Upon publication, the government abided by its pledge to restrict the range of sensitive data contained in the database. Rather than targeting the "opinions" of "public personalities", it now spoke of the "public activities" of people that might threaten public security. But as the journalist and privacy expert Jean-Marc Manach then observed, the wording remained vague. In his words, PASP was still a "database on "presumption" (Leloup, 2009).

A few years later, another intelligence crisis led to a new expansion of PASP. In 2009, following the spectacular outbreak of the Yellow Vests protests, the intelligence services were told to identify the "leaders" of this highly decentralised social movement – in particular through data drawn from social networks – apparently by using PASP. In mid-2020, after the National Strategy on Intelligence made the surveillance of social movements a key priority (Présidence de la République, 2019) the government submitted draft decrees to legalise ex post this extralegal surveillance operation (Guiton, 2020). However, whilst doing so, it also reintroduced in PASP many of the categories of data that were found in EDVIGE in 2008, including political opinions, health data, and information on minors. The CNIL had asked the government to "explicitly exclude the possibility of automated collection" of data from social networks in this new decree. Once again, however, the government chose to ignore the privacy watchdog. As of 2020, the PASP database contained more than 60,000 individual files (Buffet, 2021). As for the Council of State, it rejected the legal challenges mounted against the expansion of PASP, just as it had rejected those against EDVIGE.

References

Batho, D., & Bénisti, J.-A. (2011). *Rapport sur la mise en oeuvre des conclusions de la mission d'information sur les fichiers de police* (n° 4113). Assemblée Nationale, Commission des Lois. https://www.assemblee-nationale.fr/13/rap-info/i4113.asp#P502_109814

Buffet, F.-N. (2021). *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2020-2021* (Délégation Parlementaire Au Renseignement). Parlement français. https://data.guardint.org/en/entity/lt5yiihrcv

Mafart, J. (2018). EDVIGE. In *Dictionnaire du renseignement* (pp. 327–330). Perrin.

Marzouki, M. (2009). « Non à Edvige »: Sursaut ou prise de conscience ? *Plein droit*, *80*, 21–26.

La Stratégie Nationale du Renseignement (Coordination Nationale Du Renseignement et de La Lutte Contre Le Terrorisme, p. 13). (2019). Présidence de la République. http://www.sgdsn.gouv.fr/uploads/2019/07/20190703-cnrlt-np-strategie-nationale-renseignement.pdf

Tréguer, F. (2017). Intelligence Reform and the Snowden Paradox: The Case of France. *Media and Communication*, *5*(1), 17–28. https://doi.org/10.17645/mac.v5i1.821

Media archives

Chemin, A. (2008, September 2). La colère associative monte contre Edvige, le fichier policier de données personnelles. *Le Monde.fr*. https://www.lemonde.fr/societe/article/2008/09/02/la-colere-associative-monte-contre-edvige-le-fichier-policier-de-donnees-personnelles_1090552_3224.html

Guiton, A. (2020, December 10). *L'exécutif lâche la bride aux fichiers de renseignement territorial*. Libération. https://www.liberation.fr/france/2020/12/10/l-executif-lache-la-bride-aux-fichiers-de-renseignement-territorial_1808254/

Piquemal, M. (2008, September 10). *Quand un organe de l'ONU épinglait Edvige*. Libération. https://www.liberation.fr/france/2008/09/10/quand-un-organe-de-l-onu-epinglait-edvige_23733/

Leloup, D. (2009, October 20). Edvige 2 est un fichier de présomptions. *Le Monde.fr*. https://www.lemonde.fr/societe/article/2009/10/20/edvige-2-est-un-fichier-de-presomptions_1256456_3224.html

Les services de renseignement pourront ficher les mineurs de plus de 13 ans. (2008, July 1). Le Monde. https://www.lemonde.fr/societe/article/2008/07/01/les-services-de-renseignement-pourront-ficher-les-mineurs-de-plus-de-13-ans_1065193_3224.html

DE 2008-12-08: The ANSO Affair

On the 6th of December 2008, Spiegel published a short article on the alleged surveillance of the Afghan NGO-Safety Office (ANSO) by the Bundesnachrichtendienst (BND). The office was financed and organised by the German NGO "Welthungerhilfe". The article disclosed that BND admitted to the Welthungerhilfe that they collected up to 2000 "telecommunications" of the ANSO office between October 2005 to April 2008. The case sparked outrage but there were no consequences on the oversight of the practices of the BND.

Starting point: The affair became public with a short article published by *Spiegel* on the 6th of December 2008. The article revealed that a German funded NGO, the Afghanistan NGO-Safety Office (ANSO), became subject to surveillance by the BND. The "Welthungerhilfe", an well-established German NGO acting as the patron of ASNO, released a press release two days after the article. They condemned the surveillance by the BND. The BND on the other hand argued that the surveillance was carried out "(…).for the purpose of detecting and countering international terrorist attacks" and the evaluation of the information to "assess the general security situation in Afghanistan" as reported by news outlets (Welthungerhilfe, 2008). In total, the responsible BND department stored and evaluated at least 2000 telecommunications from an internal distribution list of the ANSO.

Wider intelligence-related context: *Spiegel* speculated that the likely reason for the surveillance of the ANSO was the "seismographic" properties of the office. Meaning, that on the basis of the information exchanged in the ANSO, a relatively accurate and up-to-date assessment of the security situation in Afghanistan could be made. This was considered to be one of the motives of the BND. The Welthungerhilfe met the incident with "disgust". They claimed that the operation jeopardised the credibility of the office and worsened the prospects of humanitarian work. A key point of controversy was the fact that some of the employees at the office were German citizens and as such enjoy a certain degree of protection in their telecommunication; according to the 10th article of the German constitution. However, the "G10 Commission", an oversight body approving surveillance measures, approved the operation and thus the surveillance of German citizens. In a protocol of the inquiry of the German Parliament "Bundestag" regarding the NSA-Scandal, it is explicitly stated that the surveillance request was accepted by the G10 (German Bundestag, 2014, 83).

Within the debate in the inquiry, where an intelligence officer was interrogated on the general surveillance practices of the BND, a controversy was sparked by opposition parties regarding the classification of citizens as “Funktionsträger” (functionaries). The dialogue in the inquiry hinted that functionaries can be excluded from the constitutional protection of personal communications and that this classification was arbitrarily applied to German employees of the Welthungerhilfe by the BND to enable the surveillance (German Bundestag, 2014)

Transnational dimension: The ANSO acted as an umbrella for several Western non-governmental organisations that were active in Afghanistan at that time. Furthermore, it was well connected to civil society in Afghanistan and Kabul and accommodated findings of several aid organisations. The office maintained field offices in four Afghan provinces and was financed by the European Union. The surveillance of the ANSO cost the office significant reputational damage, especially on the side of the Afghanis. As director of the ANSO, Nic Lee put it: “This undermines trust in us. We will have a harder time getting information from other non-governmental organisations if you have to be afraid of being bugged” (Welthungerhilfe, 2008).

Change in oversight: In retrospect, the incident is viewed as a mistake. Harald Fechner, another witness in the NSA inquiry of the Bundestag, considered the ANSO case as an example on how the BND makes mistakes and how it should not be seen as a deliberate intention of overstepping the law (German Bundestag, 2015). However, other than bad publicity and some side references in other inquiries, no changes in oversight could be observed. The functionary assignment was later declared unlawful by the German Constitutional Court and some reforms were thus made (Bundesverfassungsgericht, 2020). However, due to the relatively low levels of attention the case received, it would be too far-fetched to argue that the ANSO case contributed solely to this reform. Rather, the case demonstrated the general apathy of the German public towards abuses of intelligence powers at that time, especially when surveillance targets were abroad. Opposition politicians criticised the BND and accused it of considering foreign countries to be a space free of fundamental rights (Lorscheid, 2008).

References

Deutscher Bundestag. (2014, November 6). *Stenographic protocol of the 20th session.* https://dserver.bundestag.de/btd/18/CD12850/D_I_Stenografische_Protokolle/Protokoll%2020%20I.pdf

Constitutional Court’s decision 1 BvR 2835/17 (2020, May 19). https://www.bundesverfassungsgericht.de/SharedDocs/Downloads/DE/2020/05/rs20200519_1bvr283517.pdf?__blob=publicationFile&v=3

Welthungerhilfe (2008, December 8). *Press release: Welthungerhilfe outraged by BND wiretapping operation*. Nachdenkseiten. https://www.nachdenkseiten.de/upload/pdf/PM-BND.pdf

Deutscher Bundestag (2015). BND-Zeuge Fechner weist Vorwürfe zurück. Archiv des deutschen Bundestages. https://www.bundestag.de/webarchiv/textarchiv/2015/kw12_pa_1ua-365136

Media archives

BND spähte deutsche Entwicklungshelfer aus. (2008, December 6). *Spiegel Online.* https://www.spiegel.de/politik/ausland/afghanistan-bnd-spaehte-deutsche-entwicklungshelfer-aus-a-594861.html

German Intelligence Admits to Spying on Charities in Afghanistan (2008, December 7). *Deutsche Welle*.

https://www.dw.com/en/german-intelligence-admits-to-spying-on-charities-in-afghanistan/a-3855839

Lorscheid, H. (2008, December 30). Eskapaden und Aktivitäten des BND 2008. *Heise Online.* https://www.heise.de/tp/features/Eskapaden-und-Aktivitaeten-des-BND-2008-3421290.html

Porteck, S. (2008). Deutsche Entwicklungshelfer vom BND ausgespäht. *Heise online*. https://www.heise.de/newsticker/meldung/Deutsche-Entwicklungshelfer-vom-BND-ausgespaeht-187097.html

FR 2010-11-13: The Squarcini affair

In September 2011, the French press revealed that the DCRI, the domestic intelligence agency, placed one of Le Monde's reporters under surveillance. At the time, then head of State Nicolas Sarkozy was embroiled in a politico-financial scandal, and Bernard Squarcini – whom he appointed at the head of the DCRI –, wanted to find the source within the government leaking sensitive information to the press. Squarcinidid so by using an old and overlooked provision of the French intelligence framework that was instrumentalised to circumvent the intelligence oversight committee's ex ante review. The scandal, which eventually led to the conviction of Squarcini for illegal surveillance, illustrates how a broadly-worded provision can be secretly interpreted to engage in illegal surveillance.

Starting point: In its edition dated 13 September 2010, Le Monde announced its intention to sue the government for violating the confidentiality of one of its journalists' sources. The government of president Nicolas Sarkozy was then embroiled in an important scandal around the illegal funding of the ruling conservative party by billionaire heiress Liliane Bettencourt. As it would later turn out, the French presidency had realised that high-level governmental sources were leaking information to the press regarding ongoing investigations on the Bettencourt affair. To identify these sources, the DCRI – the domestic intelligence agency – reached out to the telecom provider of Le Monde's journalist, Gérard Davet, demanding access to his cell phone metadata.

In response to Le Monde's disclosures on this surveillance operation, high-level officials at the Ministry of the Interior – including Bernard Squarcini, director of the DCRI – claimed that the authorities had intervened "as part of its mission to protect institutions" and spoke of mere "technical checks" carried on Davet's phone logs conducted after the ex ante review of the oversight agency, the National Commission for the Control of Security Interceptions (CNCIS) (Kauffmann, 2010). The head of the CNCIS, Rémi Récio, was quick to deny and debunk these claims, stressing instead that according to the 2006 law legalising intelligence access to metadata, such requests could only be admissible "in the context of the prevention of terrorism," which was obviously not the case in this specific instance.

Wider intelligence-related context: Le Monde's complaint came at a time of an increased politicisation of intelligence agencies. President Nicolas Sarkozy had placed his loyal allies, like Squarcini, to the heads of the agencies. Sarkozy had apparently personally supervised the surveillance of journalists deemed hostile to his presidency by issuing direct orders to Squarcini (Le Monde, 2010b). The revelation of the DCRI's illegal surveillance came as an embarrassment for the government, which kept denying any wrongdoings despite mounting evidence to the contrary. In November 2010, when the issue reached the floor of the National Assembly, Prime Minister François Fillon claimed that intelligence surveillance was conducted with "strict respect for public liberties". "The truth," he alleged, "is that there is no plot; there is only the national interest". Interior Minister Brice Hortefeux told the deputies that "the DCRI [was] not the STASI". Another government minister, Nathalie Kosciusko-Morizet, spoke of the surveillance of journalists as "an old French fantasy" relayed by the media. As for Bernard Squarcini, he denied being interested in the surveillance of journalists: "The only journalists I am interested in are those who are involved with foreign services" he told reporters (Lhomme, 2011).

On the legal front, the French government argued that the surveillance of Davet could have legally been conducted under article 20 of the 1991 Wiretapping Act. But this seemed anachronic at best – when article 20 was passed, the DGSE was still in the midst of a major infrastructural upgrade to develop its bulk satellite surveillance capabilities. These capabilities were given a blank check through this provision, which stated that "measures taken by public authorities to ensure, for the sole purpose of defending national interests, the surveillance and the control of Hertzian transmissions" were not subject to the procedural safeguards laid out in the law. "National interests" and "Hertzian transmissions" remained undefined, but nobody in

parliament seemed to care. In 1999, the CNCIS had made clear in its 1999 report that article 20 could only be used for "the defence of national interests" and that it excluded any search for "individualised communications" (CNCIS, 2000).

In the course of the 2010s, several disclosures would show that the 2010 spying of Le Monde's reporter was just one of the many illegal surveillance activities retrospectively justified by this blank check provision (Tréguer, 2016). Not only was it used as a legal basis for the surveillance of international satellite transmissions, as originally intended; it also served as legal basis for the domestic surveillance of WiFI, GSM, and GPS communications, as well as the large-scale internet surveillance program rolled out by the DGSE from 2008 onwards. Key officials also hinted at rampant abuse. For instance, former member of parliament Jean-Jacques Hyest, who had taken part in the legislative debate over the 1991 Wiretapping Act and sat on the oversight commission from 2010 to 2014, regarding the extra-legal surveillance of a political opponent of former President Sarkzoy, was quoted in 2016 as saying: "I have always said that it was unbearable to use article 20 for all and everything" (Follorou, 2016). In 2013, Jean-Jacques Urvoas, then member of parliament, called article 20 "the grey zone" that epitomised "the government's inability to keep in check the methods of the [intelligence] services" (Kallenborn, 2013).

In 2010, the resort to article 20 to shield illegal surveillance operations was not news either. As a matter of fact, as early as 2009, the CNCIS had alerted the Prime Minister's office that the provision was used illegally to access telecommunications metadata outside of the restricted scope of anti-terrorist investigations. Jean-Louis Dewost, then-head of the CNCIS, said that in 2009, "during a control procedure on the premises of a telephone operator, we realised that requests for 'fadettes', and then wiretaps, were made directly via article 20 of the 1991 law, without going through the commission that I chaired" (Le Monde, 2010a). Not only did these findings yield no sanction, but they did not receive publicity and were completely disregarded.

Change in oversight: Although the Squarcini affair came as a proof that the legal framework for intelligence surveillance was becoming obsolete and that oversight mechanisms were failing, there was no convincing attempt at remedying the situation with new legislation. Government officials sued several newspapers accusing them of defamation for documenting the affair. Meanwhile, several journalists working on the Bettencourt affair had their computers mysteriously stolen. Le Monde's complaint followed its course despite attempts of the government to block the investigation by invoking state secrets (Bordenave, 2010). Squarcini eventually lost the case in 2014, when a Paris court ruled that such surveillance could not be used for the targeted surveillance of an individual. He was sentenced to a €8000 fine – a lenient sanction which the prosecutor had deemed necessary to "take into account the services rendered by Mr. Squarcini to the Republic" (Mediapart, 2014).

As for article 20, it survived the major legislative reform enacted in the post-Snowden context to update the antiquated 1991 Wiretapping Act. During the parliamentary debate on the Intelligence Act in the Spring of 2015, the numerous opponents both inside and outside of parliament hadn't realised that, amidst all the legalese, the text simply relocated article 20 under article L. 811-5 of the Code of Interior Security. It is only by chance that article 811-5 was "rediscovered" in April 2016 following a report from *Le Monde* on the above-mentioned case of political spying. The article was published just as a volunteer litigation team tied to civil society organisations was wrapping up its legal briefs against the implementation decrees of the Intelligence Act (filed before the Council of State, France' supreme administrative court) (Tréguer, 2016). The subsequent constitutional challenge led to a ruling by the Constitutional Council in October 2016 which struck down the provision, giving time for the government to pass a legislative patch that secured a detailed legal basis for bulk surveillance of satellite interceptions. This closed a blatant, 25 year-old loophole in the French intelligence framework.

References

Commission nationale de contrôle des interceptions de sécurité. (2000). *8e rapport d'activité (1999)*. CNCIS.

Tréguer, F. (2016, October 26). French Constitutional Council Strikes Down "Blank Check Provision" in the 2015 Intelligence Act. *Verfassungsblog*. http://verfassungsblog.de/french-constitutional-council-strikes-down-blank-check-provision-in-the-2015-intelligence-act/

Media archives

Affaire des fadettes: Squarcini condamné à 8000 euros d'amende. (2014, April 8). *Mediapart*. https://www.mediapart.fr/journal/france/080414/affaire-des-fadettes-squarcini-condamne-8000-euros-damende

Bordenave, Y. (2010, October 9). Affaire des écoutes du 'Monde': Le secret-défense invoqué. *Le Monde*. https://www.lemonde.fr/societe/article/2010/10/09/affaire-des-ecoutes-du-monde-le-secret-defense-invoque_1422968_3224.html

Follorou, J. (2016, April 12). Comment la DGSE a surveillé Thierry Solère. *Le Monde*. http://www.lemonde.fr/societe/article/2016/04/12/comment-la-dgse-a-surveille-thierry-solere_4900451_3224.html

Kallenborn, G. (2013, August 28). *La DGSE exploite un article de loi pour aspirer légalement nos métadonnées*. 01net. https://archive.ph/x7nmM

Kauffmann, S. (2010, September 20). Secret des sources: Ce que dit la plainte du 'Monde'. *Le Monde*. https://www.lemonde.fr/politique/article/2010/09/20/la-plainte-du-monde-pour-violation-du-secret-des-sources-deposee-au-parquet-de-paris_1413744_823448.html

Lhomme, F. (2011, September 1). Affaire Bettencourt: Les services secrets ont espionné un journaliste du 'Monde'. *Le Monde*. https://www.lemonde.fr/societe/article/2011/09/01/affaire-bettencourt-les-services-secrets-ont-viole-le-secret-des-sources_1566033_3224.html

Selon 'Le Canard enchaîné', Sarkozy supervise l'espionnage de journalistes. (2010a, November 2). *Le Monde.fr*. https://www.lemonde.fr/politique/article/2010/11/02/selon-le-canard-enchaine-sarkozy-supervise-l-espionnage-de-journalistes_1434560_823448.html

Surveillance téléphonique: Matignon alerté depuis la fin 2009. (2010b, November 14). *Le Monde.fr*. https://www.lemonde.fr/politique/article/2010/11/14/surveillance-telephonique-matignon-alerte-depuis-la-fin-2009_1439889_823448.html

UK 2013-08-18: The Detention of David Miranda

In August 2013, David Miranda was detained for nine hours at Heathrow airport, under Schedule 7 of the Terrorism Act 2000. Miranda, the partner of Glenn Greenwald (a journalist who was leading on the Snowden revelations), was arrested whilst in transit on a journey from Berlin to Rio De Janeiro. Upon his detention, the police seized all technological devices. Miranda's passport was held for a further three hours after his detention of nine hours. Matthew Ryder QC, who represented Miranda in court described this use of Schedule 7 to seize journalistic material to be possibly the first of its kind. Much of the outrage around the scandal was concerned with the protection of journalists, and the scope of powers available to authorities under anti-terrorism legislation. Miranda challenged his detention in the High Court which ruled it justifiable, but later won a partial victory in the Court of Appeal in 2016.

Starting point: Miranda was returning to Rio De Janeiro after meeting Laura Poitras, who had worked with Miranda's partner Glenn Greenwald on the Snowden revelations from June 2013. In his transit from Berlin, at Heathrow airport, Miranda had his equipment confiscated, and was detained for 9 hours (the maximum time given under schedule 7 before an arrest or release must be made), having access to his solicitor after 8 hours in detention (Miranda, 2017). Many highlighted the extreme conditions of his detention and pointed to official figures that showed "most examinations under schedule 7 – over 97% – last less than an hour, and only one in 2,000 people detained are kept for more than six hours" (Guardian Staff, 2013). Miranda's detention put a spotlight on the implementation of anti-terrorism legislation, and by his own account (Miranda, 2017), the radicalracialised way it is implemented. The discussion that arose from David Miranda's detention centred around the protection of journalists and journalistic material.

Wider Intelligence-related context: The scandal is clearly linked to the Snowden revelations in 2013 (see Snowden section), but the use of anti-terrorism legislation (instead of for example the Official Secrets Act) in detaining Miranda, meant that this scandal also tapped into intelligence issues beyond and before Snowden's revelations. Describing Miranda's detention, the then director of Liberty, Shami Chakrabarti (quoted in 2013 in O'Carroll and Norton-Taylor, 2013) said that the detention:

> […] was possible due to the breathtakingly broad schedule 7 power, which requires no suspicion and is routinely abused…People are held for long periods, subject to strip searches, saliva swabbing and confiscation of property – all without access to a publicly funded lawyer. Liberty is already challenging this law in the court of human rights but MPs disturbed by this latest scandal should repeal it without delay.

Schedule 7 came after Section 44 of the Terrorism Act which had previously garnered similar criticisms, and its wide scope was part of why it had been ruled unlawful by the European Court of Human Rights (Kennedy, 2014). Miranda's detention was even criticised by Falconer, who was a lord chancellor that had helped pass the Terrorism Act in the House of Lords (Watt, 2013).

Defending the Home Secretary in the legal challenge brought forward by Miranda, Steven Kovats QC argued that the Home Secretary submitted that Snowden's material "was capable of being an act of terrorism", justifying the detention of Miranda under Schedule 7 (BBC, 2013). This raised much discussion about the scope of anti-terrorism legislation. Miranda's release after nine hours of detention raised questions about the classification of "terrorist activity" by the Home Secretary, especially given that he was not arrested post-detention.

The scandal exposed how different domestic (and international) agencies and authorities were working collectively (including for example agencies of police, border, government, security services). The assertion by then Home Secretary Theresa May that this was an independent decision by the police was doubted, given her briefing before the detention, as well as the White House being notified beforehand. The independence of the police on this detention was also doubted given their persuasion for grounds of detention (which did not initially exist on their part) but was provided via the Port of Circulation Sheet offered by Security Services (Owen, 2013). The ability to process the data would also require the involvement of other agencies, including foreign agencies (Robbins, 2013).

Transnational: The scandal was bound to be transnational, given the detention of a Brazilian national by UK authorities. Miranda (2017) in fact cites the role of his nationality, identity, and language skills in his detention. A hostile response from Brazilian authorities who saw Miranda's detention as unjustifiable was expected.

In terms of the data, it is important to remember that Snowden's revelations contained information on global surveillance systems. The confiscation of Miranda's equipment was therefore likely to be in the interest of actors beyond UK intelligence agencies (particularly the NSA), and the reason why the White House was given a "heads up" before David Miranda's detention (Watt and Gabbatt, 2013). However, the deputy press secretary for the White House, Josh Earnest, distanced the US from the detention of Miranda claiming that "This is a decision that was made by the British government without the involvement – and not at the request – of the United States government" whilst acknowledging that the US government was told beforehand that the detention was "likely to occur" (Earnest in Watt and Gabbatt, 2013).

In Oliver Robbins (then-Deputy National Security Adviser for Intelligence, Security, and Resilience in the Cabinet Office)'s witness statement, he expanded on the exchange of information between the police and UK intelligence agencies under section 19 of the Counter-Terrorism Act of 2008 (Robbins, 2013). Although caveating disclosure of information with foreign parties, Robbins (2013) shed light on the sharing and retention of data, which of course has transnational dimensions:

> The UK intelligence agencies may, in turn, disclose this information to a third party, including selected foreign parties, in the exercise of their statutory functions. It may well be necessary to

> disclose or provide access to the material seized by the police to foreign third parties to support the UK intelligence agencies' ability to access and to interpret the electronic media (Robbins, 2013, p.10).

Changes to oversight: Much of the outrage that followed the detention of Miranda was around the protection of journalists, and journalistic material. Loud condemnations came from various outlets (e.g. from the National Union of Journalists, Society of Editors, English PEN) championing protections for journalists and the associated freedoms of expression, especially sacred for journalists. A written intervention was given by Article 19, English PEN, and the Media Legal Defence Initiative in the legal challenge brought by Miranda. European editors also wrote an open letter to David Cameron describing their concern, especially with regard to free press, and the effects of this detention that will be felt beyond the UK (Doward, 2013). Oversight was therefore arguably being exercised by non-parliamentary actors.

Within the parliamentary sphere, debates saw Conservative MP Peter Tapsell asking David Cameron about oversight of the security services (Owen, 2013), and Caroline Lucas tabling an Early Day Motion 1021 in January 2014. The EDM stated that "Schedule 7 of the Terrorism Act 2000 is being illegitimately used to undermine freedom of the press; and calls on the Government urgently to review the application of the Terrorism Act 2000 and guarantee that it is not used to intimidate or persecute national security journalists" (Lucas, 2014), but only garnered 21 signatures. Similarly, the then independent reviewer of terrorism legislation, David Anderson's criticism and report, although cited widely, was limited when it came to implementing changes in legislation.

Whilst the High Court ruled in favour of the government in 2014, the ruling was partially overturned in the Court of Appeal in 2016. Whilst upholding the detention to be lawful, the ruling argued that stop laws for the acquisition of journalistic material were incompatible with Article 10 of the European Convention of Human Rights.

References

Between: Claimant: REGINA (DAVID MIRANDA)—And—Respondents: (1) SECRETARY OF STATE FOR THE HOME DEPARTMENT, (2) COMMISSIONER OF POLICE OF THE METROPOLIS; Interveners: (1) LIBERTY (2) ARTICLE 19, ENGLISH PEN AND THE MEDIA LEGAL DEFENCE INITIATIVE, The Court of Appeal (Civil Division) on Appeal form the High Court, Case No: C1/2014/0607 (2016). https://www.judiciary.uk/wp-content/uploads/2016/01/miranda-v-home-sec-judgment.pdf

Between:David Miranda (Claimant) -and- The Secretary of State for the Home Department (1st Defendant), The Commissioner of the Police of the Metropolis (2nd Defendant) -and- (1) Liberty (2) English Pen, Article 19 & Media Legal Defence Initiative (3) Coalition of Media & Free Speech Organisations (Interveners), The High Court of Justice Divisional Court, Case No: CO/11732/2013 (2014).

First Witness Statement of Oliver Robbins, High Court of Justice, CO/11732/2013 (2013).

Port Examination Codes of Practice and National Security Determinations Guidance Regulations 2020, no. Volume 804 (2020).

The royal society for arts, manufactures and commerce (RSA). (2017, September 19). An Evening with Glenn Greenwald and David Miranda. https://www.youtube.com/watch?v=g1McjoIm_sM

Media archives

Doward, J. (2013). David Miranda's detention is a threat to press freedom, say European editors. The Observer. https://www.theguardian.com/world/2013/aug/24/david-miranda-detention-greenwald-press-editors

Edward Snowden articles 'could be acts of terror'. (2013, November 6). BBC. https://www.bbc.co.uk/news/uk-24830684

Guardian Staff. (2013). Glenn Greenwald's partner detained at Heathrow airport for nine hours. https://www.theguardian.com/world/2013/aug/18/glenn-greenwald-guardian-partner-detained-heathrow

Kennedy, H. (2014). The David Miranda judgment has chilling implications for press freedom, race relations and basic justice. The Guardian. https://www.theguardian.com/commentisfree/2014/feb/19/david-miranda-press-freedom-race-justice

O'Carroll, L., & Norton-Taylor, R. (2013, August 19). David Miranda detention prompts outcry over 'gross misuse' of terror laws. The Guardian. https://www.theguardian.com/world/2013/aug/19/david-miranda-detention-outcry-terrorism-laws

Owen, P. (2013, November 6). NSA files – David Miranda launches high court challenge. The Guardian. https://www.theguardian.com/world/2013/nov/06/nsa-files-david-miranda-high-court-challenge-live

Watt, N. (2013). David Miranda's detention had no basis in law, says former lord chancellor. The Guardian. https://www.theguardian.com/world/2013/aug/21/david-miranda-law-detention-heathrow

Watt, N., & Gabbatt, A. (2013). David Miranda detention: White House was given 'heads-up'. https://www.theguardian.com/world/2013/aug/19/white-house-david-miranda-heads-up

FR 2013-11-20: The LPM Debate on Metadata Surveillance

On October 14th 2013, the tech-focused online media NextInpact published an analysis of "article 13" of the French Military Planning Bill, which was making its way through Parliament and aimed at expanding intelligence access to metadata. Strangely in a context marked by the global Snowden disclosures, no one in the advocacy sphere seemed to take notice. On November 20th, the French lobby for the tech sector ASIC finally reacted to article 13 through a press release calling for a moratorium on new surveillance measures. This unexpected denunciation sparked a short and unsuccessful mobilisation by human rights organisations to defeat article 13, which effectively legalised ongoing practices. By demonstrating the unpreparedness of the French civil society regarding intelligence surveillance policy, the scandal acted as a wake-up call. As a consequence, a group of NGOs decided to set up new coordination channels and build shared expertise on the issue through establishing a new umbrella organisation entitled Observatoire des Libertés et du Numérique (OLN).

Starting point: On October 14th 2013, the tech-focused online media NextInpact published an analysis of "article 13" of the Military Planning Bill, which had recently been amended by the Senate. In the midst of the global surveillance scandal unleashed by Edward Snowden, journalist Marc Rees wrote, the centre-left majority in Parliament had decided to team up with the socialist government of President François Hollande to pass new legislation expanding access by intelligence agencies to the troves of telephone and Internet metadata retained by hosting and access providers.

Wider intelligence-related context: Through a 2006 reform, French intelligence agencies were authorised to request telecom operators to hand over metadata retained on their users, but for the sole purpose of fighting terrorism. Other purposes like economic espionage or monitoring social movements remained out of the provision's scope. But as it would later surface through parliamentary reports published ahead of the adoption of the 2013 Military Planning Bill, French intelligence was quick to find a loophole to override those restrictions: under the veil of secrecy, intelligence officials had successfully used article L. 244-2 of the 1991 Wiretapping Law – which allowed intelligence services to request metadata to make preparations for an interception – to access metadata in all kinds of circumstances beyond anti-terrorism, with no independent oversight (Urvoas & Verchère, 2013, p. 24). Also, from 2009 on, intelligence agencies had apparently experimented with traffic-scanning devices provided by Qosmos and installed on the infrastructure of major telecom operators to monitor metadata in real-time (Hourdeaux, 2016). One key objective of the 2013 Military Planning Act reform was to expand the scope of metadata requests to the whole spectrum of intelligence policy goals and to legalise such real-time access to both metadata and geolocation data. Compared to the government's original proposal, the Senate version of article 13 brought a few oversight mechanisms.

Although the reform had actually been addressed quite at length in parliamentary reports in the upcoming months, the news around this legalisation process of illegal surveillance capabilities did come as a surprise to many in the advocacy sphere. Initially, almost no one reacted to Rees' piece, and no human rights group

seemed to care. It was only five weeks later, on November 20th, that the *Association des services de l'Internet communautaire* (ASIC) – a professional lobbying organisation representing online social services including Google France, AOL, eBay, Facebook, Microsoft, Skype and French companies like Deezer or Dailymotion – released a brief on article 13. Their concerns were relayed in the right-wing newspaper Le Figaro, with a sensationalist article entitled: "Telephone, Internet: The State Will Soon Be Able to Spy on Everything" (Leclerc, 2013). In turn, this led to growing media attention to the provision in many media's tech sections. On December 3rd , the Minister of Digital Affairs, Fleur Pellerin, was interviewed in *Le Monde* (Follorou & Johannès, 2013). The interview's headline stressed that she was "the first member of the government to react to surveillance of the digital sphere." In the interview, Pellerin introduced what would become an important justification in the coming months in intelligence policy and cybersecurity debates, framing the Snowden disclosures –which had documented the role of Silicon Valley corporations in US surveillance programs– as a confirmation that these "hegemonic" private actors were a major threat for privacy and broader European interests, casting their defence of digital rights in France as a sign of their double-dealing on the issue.

However, on the same day, the leading (though relatively small) French digital rights advocacy group, La Quadrature du Net finally reacted with a press release denouncing article 13: "How is it possible," it asked, "that after only a few months of Edward Snowden's revelations the French government proposes a bill so detrimental to our fundamental rights?". The day after, the Digital Economy Council, a government advisory body, also came out strongly against the provision (Conseil national du numérique, 2013). From there on, many organisations joined this late but dense opposition. On December 9th, as the bill went back to the Senate floor in second-reading, major human rights organisations joined the mobilisation. The Ligue des droits de l'Homme (LDH) for instance called on the Parliament to delete article 13. On December 10th, Reporters Without Borders denounced its impact for the confidentiality of reporter's sources, as well as the lack of consultation on the provision. But on that day, despite the growing mobilisation by civil society and media attention to the issue, and despite an increasingly vocal opposition by a few MPs, the French Parliament definitively adopted the Military Planning Law.

Changes in oversight: Despite its somewhat exaggerated denunciation of "generalised surveillance" and its failure to block article 13, this first episode of post-Snowden contention had at last led to a process of mobilisation around Internet surveillance by intelligence agencies. On the web page of an unsuccessful petition calling for referral to the Constitutional Council, an update was added to stress that, "for the first time in France, our action has led to the creation of an actual movement for the protection of our freedoms on the Internet." This may have been an overstatement, as there had been prior wide ranging mobilisations. But in recent memory, such a mobilisation against Internet surveillance by intelligence agencies – even though it was largely improvised and resulted from immediate circumstances – was indeed a first. And it would bear fruition in the longer term.

Probably frustrated by their failure to react in time to the amendments (and to do so before rather than after industry groups like ASIC) – also finally realising the need to build and share expertise around Internet surveillance and digital rights in general, and intelligence surveillance in particular–, civil society groups created creation a new umbrella organisation. Announced on the international "data protection day," it was called the Observatoire des Libertés et du Numérique (OLN). OLN's initial members included organisations that often worked together on non-Internet issues – including LDH, a lawyers union (Syndicat des avocats de France) and a judges union (Syndicat de la magistrature). They were joined by two smaller research organisations devoted to the interplay of the digital sphere and privacy (CECIL and CREIS-Terminal). A few days later, La Quadrature du Net – with its already established record on digital rights, its singular Internet-inspired political culture as well as its own international networks –, asked to join the coalition, thus becoming a new member of OLN. This new alliance would play a key role against the 2015 Intelligence Bill (Tréguer, 2017).

References

Tréguer, F. (2017). Intelligence Reform and the Snowden Paradox: The Case of France. *Media and Communication*, *5*(1), 17–28.

Urvoas, J.-J., & Verchère, P. (2013). *Rapport en conclusion des travaux d'une mission d'information sur l'évaluation du cadre juridique applicable aux services de renseignement* (Commission Des Lois No. 1022). Assemblée nationale. http://www.assemblee-nationale.fr/14/controle/lois/renseignement.asp

Conseil national du numérique. (2013). *Avis n°5-2013 du Conseil national du numérique sur les libertés numériques*. Conseil national du numérique. http://www.cnnumerique.fr/libertes-numeriques/

Media archives

Follorou, J., & Johannès, F. (2013, December 4). Fleur Pellerin: « Big data peut devenir Big Brother, et nous essayons de résister à cela ». *Le Monde*. http://www.lemonde.fr/international/article/2013/12/04/big-data-peut-devenir-big-brother-et-nous-essayons-de-resister-a-cela_3525180_3210.html

Hourdeaux, J. (2016, June 6). *Comment les services de renseignement ont mis en place une surveillance générale du Net dès 2009*. Mediapart. https://www.mediapart.fr/journal/france/060616/comment-les-services-de-renseignement-ont-mis-en-place-une-surveillance-generale-du-net-des-2009

Leclerc, J.-M. (2013, November 25). *Téléphone, Internet: L'État pourra bientôt tout espionner*. Le Figaro. http://www.lefigaro.fr/actualite-france/2013/11/25/01016-20131125ARTFIG00570-telephone-internet-l-etat-pourra-bientot-tout-espionner.php

Rees, M. (2013, October 14). *Terrorisme et données de connexion: Fin du provisoire, des garanties…* NextInpact. http://archive.ph/ufosS

UK 2015-11-1: Controversy around the Investigatory Powers Act

In November 2015, the UK Home Secretary Theresa May published a Draft of the Investigatory Powers Bill, later passed as the Investigatory Powers Act (IPA) in December 2016. Commonly dubbed as the "Snooper's Charter" because of its extensive surveillance powers, and described by the Don't Spy on Us coalition as the "most draconian surveillance law in our history" (2016), the Act codified many controversial powers of government agencies. These included equipment interception (hacking), bulk powers of data collection, and internet connection collection methods (described by May as "simply the modern equivalent of an itemised phone bill". Opposition and oversight took on different forms (including a petition, legal challenges, public campaigns) and involved several groups within and beyond parliament, using different lines of argument in rejecting this legislation.

Starting point: Although according to May (2015), the Bill published in November 2015 was "not a return to the draft Communications Data Bill of 2012" (also dubbed the Snooper's Charter) that had been opposed by then coalition partners Liberal Democrats, much of the powers outlined in the 2015 Draft Investigatory Powers Bill were similar. May on the one hand argued that this Bill was completely new, but on the other, affirmed that much of these powers have been available to security agencies for years, citing for example Section 94 of the Telecommunications Act 1984. Important also in the passing of this legislation was the previous ruling that sections 1 and 2 of the Data Retention and Investigatory Powers Act (DRIPA) of 2014 were unlawful, meaning that new legislation needed to be proposed. This Bill was then a way to renew and amend legislation, and arguably push through legislation that would have not been possible under a coalition government.

Wider intelligence-related context: The Bill followed and in many ways confirmed Snowden's revelations, particularly in terms of bulk powers. It was published shortly after the Conservatives came into power with a majority in May 2015, having previously held power only by being in coalition with the Liberal Democrats. The Investigatory Powers Act set out various powers allowing the security services, police forces, and in the case of internet connection records, 48 agencies, to access data. These 48 agencies that had authority and would not require a warrant to access internet connection records were extensive and included, for example, the Department for Work and Pensions, HM Revenue & Customs, the Department of Health, the Food Standards Agency.

The powers set out in the Act extended to various parts of intelligence gathering/surveillance and included powers for: equipment interference (hacking), undermining of encryption (demanding government be informed of encryption methods that are wished to be used in the future and ways of circumventing encryption), internet connection records collection, and the use of bulk powers in data collection and extraction. Whilst the publication of the Bill saw a revival of a debate between privacy and security, opposition to the Bill saw various arguments adopted, and actors and politicians of different political traditions working together. Considering the Snowden revelations and the detention of David Miranda (see above), there is maybe little surprise that much opposition focused on the (lack) of protection of journalists, whistleblowers, and lawyers, although of course, the effects would not be limited to these roles and professions.

Transnational elements: Transnational effects of the Bill were rarely touched upon (King 2016). Little was said, for example, about potential data sharing with other agencies, as is commonly practised between GCHQ and the NSA, or the consequences on the rights of those residing outside the UK and how the Act would affect them when their data passes through the UK and is processed by UK actors.

Its powers were described as "unmatched by any other country in western Europe or even the US" (MacAskill, 2016), the Investigatory Powers Act was seen as exceptional in its scope. Much debate and opposition focused on comparisons with authoritarian states, referencing for example that the Chinese government "pointed to legislation proposed in Western nations, such as Britain's draft investigatory powers bill" when proposing anti-terror legislation in 2015, dubbed also as a 'Snooper's Charter' (Hern, 2015). Upon the publication of the Bill, Snowden had tweeted that "The UK has just legalised the most extreme surveillance in the history of western democracy. It goes further than many autocracies" (Snowden in MacAskill, 2016).

Gathering global attention, William E. Binney, former technical director of the NSA was invited to give evidence to the Draft Investigatory Powers Bill Committee that was set up and contributed to discussion amongst campaign groups and reports on the dangers of the Bill.

Oversight changes: Upon unveiling the Bill in November 2015, Theresa May suggested it was "world leading" in its oversight means. In her speech, May (2015) pointed to the appointment of an independent Investigatory Powers Commissioner as a form of oversight. This role would replace the roles of three previous Commissioners (Interception of Communications Commissioner, the Intelligence Services Commissioner and the Chief Surveillance Commissioner) which raised questions on the ability to oversee a vast number of authorisations. May also announced a "double lock" placed on authorisations, with warrants issued needing the approval of both the Secretary of State and a judge. A Joint Committee on the Draft Investigatory Powers Bill was set up and was arguably a form of oversight for the legislation proposed. Although evidence sessions included the questioning of different parts of the Bill, it should be noted that some parts came into effect before/regardless of parliamentary scrutiny, like bulk personal datasets.

Oversight however did not simply change on a parliamentary level. Important was the role of groups like the Don't Spy On Us coalition which brought many actors of different political visions and traditions together. The coalition worked with parliamentarians by briefing MPs and suggesting amendments (all of which were rejected). One notable demand relating to oversight by the group was published before the Bill, in the wake of Snowden's revelations; it recommended the Intelligence and Security Committee to be democratically scrutinised by parliament, rather than simply answerable to the Executive. The coalition also worked with different groups, including lawyers (200 of which signed a letter regarding the Bill), and "other stakeholders including small startups, internet industry giants, trade bodies, unions, professional associations and academia to share views and co-ordinate action" (Don't Spy On Us, 2016). A petition that was signed by over 100 000 signatories was also circulated, but after the law was passed.

Legal action has been taken by various groups on different parts of the Act. In April 2018, the High Court ruled that the Investigatory Powers Act violated EU law in a challenge led by Liberty on the topic of data retention. This forced the government to pass the Data Retention & Acquisition Regulations in October that year, although loopholes were arguably still included, and whilst the threshold for acquiring data was increased, it was still contested. In 2019, the High Court ruled that "bulk powers' don't breach privacy and free expression rights and the Act does contain sufficient safeguards for journalistic and legal

communications" (Liberty, no date). This was seen as a blow to attempts at demanding greater protection and oversight to many campaigners.

The IPA saw a range of oversight methods adopted with, within, and beyond parliamentary spheres. Although transparency supposedly increased, the Bill sought to extend and legitimise controversial practices that were occurring before its publication. Whilst there was a coming together of different groups, the focus on protections of professions, and strategies of focusing on the fear of not descending into an authoritarian state like China or Russia, seemed to gain limited results.

References

Between: Claimant: The Queen (on the Application of National Council for Civil Liberties (Liberty)). – And— 1st Defendant: Secretary of State for the Home Department,2nd Defendant: Secretary of State for Foreign and Commonwealth Affairs, no. Case No: CO/1052/2017, High Court of Justice (2018). https://www.judiciary.uk/wp-content/uploads/2018/04/liberty-v-home-office-judgment.pdf

Between: Claimant: The Queen (on the Application of National Council for Civil Liberties (Liberty)). – And— 1st Defendant: Secretary of State for the Home Department,2nd Defendant: Secretary of State for Foreign and Commonwealth Affairs, Intervener :National Union of Journalists, no. Case No: CO/1052/2017, High Court of Justice (2019). https://www.judiciary.uk/wp-content/uploads/2019/07/Liberty-judgment-Final.pdf

Draft Investigatory Powers Bill, (2015). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/473770/Draft_Investigatory_Powers_Bill.pdf

Liberty. (n.d.). *Legal Challenge: Investigatory Powers Act*. https://www.libertyhumanrights.org.uk/issue/legal-challenge-investigatory-powers-act/

May, T. (2015, November 4). *Home Secretary: Publication of draft Investigatory Powers Bill* [Oral statement to Parliament]. https://www.gov.uk/government/speeches/home-secretary-publication-of-draft-investigatory-powers-bill

Media archives

Hern, A. (2015). China introduces its own 'snooper's charter'. *The Guardian*. https://www.theguardian.com/technology/2015/dec/29/china-introduces-its-own-snoopers-charter

King, E. (2016). Raw intelligence-sharing and the Investigatory Powers Bill. *OpenDemocracy*. https://www.opendemocracy.net/en/digitaliberties/raw-intelligence-sharing-and-investigatory-powers-bill/

MacAskill, E. (2016). 'Extreme surveillance' becomes UK law with barely a whimper. *The Guardian*. https://www.theguardian.com/world/2016/nov/19/extreme-surveillance-becomes-uk-law-with-barely-a-whimper

Schweizer, K. (2016). `Snooper's Charter' Would Make Brits Most Spied-Upon People. *Bloomberg*. https://www.bloomberg.com/news/articles/2016-02-11/-snooper-s-charter-would-make-brits-most-spied-upon-people

Snowden, E. (2015, November 4). Edward Snowden's tweets on the Snoopers Charter. https://twitter.com/Snowden/status/661950808381128704

Travis, A., Wintour, P., & MacAskill, E. (2015). Theresa May unveils UK surveillance measures in wake of Snowden claims. *The Guardian*. https://www.theguardian.com/world/2015/nov/04/theresa-may-surveillance-measures-edward-snowden

DE 2020-11-7: Operation Rubicon

From 1970 to 1993, the BND was involved in a joint operation named "Rubicon". Together with the CIA, they secretly bought a business front in Switzerland, named "Crypto AG". Crypto AG sold mechanical encryption

devices for the encryption of state communication. The intelligence agencies involved rigged the company's devices so they could easily break the codes that client countries used to send encrypted messages for their governmental communication. Within Operation Rubicon, the CIA and BND were able to read almost the entire communication of the so-called "Third World" during the Cold War through manipulated cryptographic devices that were sold to friend and foe. The scandal received little attention in Germany. However, it led to the resignation of the Chief of Swiss Intelligence.

Starting point: In July 2020 a journalist collective, consisting of Swiss SRF, German ZDF and American Washington Post, evaluated a comprehensive intelligence dossier on Operation Rubicon. They published their findings in their respective networks and media, revealing that between 1970 and 1993, Crypto AG sold manipulated communication devices to a great number of governments. It became one of the most important manufacturers of cryptographic devices in the world after WWII. However, it was disclosed that the Crypto AG had been bought in 1970 covertly by the CIA and BND after its founder had passed away without an heir to continue the business.

In the early 1990s, there had already been unproven hints that the Crypto AG could have been an intelligence operation's front. At the time, Crypto AG's Salesman Hans Bühler was arrested in Iran on a business trip. Bühler, who was not informed about the secret operation, was held for nearly one year from March 1992 to January 1993. He was released by the Iranian authorities after Crypto AG bailed him out for 1.000.000$. The money was provided by the BND covertly because Crypto AG lacked sufficient resources. The US Government rejected paying their share. Bühler became suspicious and talked to the press, accusing Crypto AG of using exploits in their codes for the benefit of German and US intelligence. A statement that would get him fired.

This in the end led to the German retreat from the Operation in 1994. As described by in the Crypto Musuem:

> "(…), there was the increasing risk of exposure. Dissidents within the company were seeking public recognition for their suspicions, and had been talking to the press on several occasions. But the real turning point was – no doubt – the Hans Bühler affair. It had made the Germans very nervous." (Crypto Museum, 2022).

Sarah Mainwaring writes:

> "Frustrated at America's reluctance to pay 'their share' of the bill, annoyed by the failure to silence Bühler, and horrified by the resulting publicity, this event raised real concerns for the few senior German politicians who were in the know about the operation"

Wider intelligence-related context: Through Crypto AG, BND and CIA were able to tap into the communication of 130 Governments and Intelligence Services worldwide. According to the Washington Post, Operation Rubicon was responsible for over 40% of "(…) the diplomatic cables and other transmissions by foreign governments that cryptanalysts at the NSA decoded and mined for intelligence" (Washington Post, 2020) and over 90% for the BND. After the operation was almost disclosed in 1993, the BND quit the operation, the CIA continued up until 2018, when digital surveillance made mechanical manipulation obsolete.

Transnational dimension: Operation Rubicon was an extremely close cooperation between the BND and CIA, even though this cooperation was not without conflict. It is a prime example for the possible dimension of interconnection and the transnationality in the field of intelligence. The US and Germany were the perpetrators, using Switzerland as a conduit to surveill other states.The revelation stirred a lot of attention in Switzerland, the country where the Crypto AG was based as the SFR broadcasted a very detailed documentation that elevated the issue on the public agenda.

The main aspect at stake was the Swiss neutrality doctrine. There are two dimensions to this point. First, it is the Swiss neutrality doctrine that was used as a selling argument for this sensible product (Aldrich et al., 2020, 2). Second, parts of the Swiss Administration and Security Services had knowledge of the operation and seemed to tolerate it. Within the Swiss Parliament a debate began on whether and to what extent Operation Rubicon has jeopardised the credibility of Switzerland as a neutral state (Mainwaring, 2020, 2).

Change in oversight: Operation Rubicon did not led to any significant public uproar or oversight adjustments in Germany. However, the affair posed a problem for Swiss executives. In May 2021, the Chief of Swiss Intelligence Jean-Philipple Gaudin resigned from his position. A report by the newspaper "Tagesanzeiger" speculated that this could be due to his restraint in informing the Swiss Government on the nature of the Crypto AG.

Media archives

Miller, G. (2020, February 11). The Intelligence Coup of the Century. *Washington Post.* https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/

ZDF (2020, August 29). *Streng geheim! Cryptoleaks. Die große BND und CIA Spionage.* Youtube. https://www.youtube.com/watch?v=jagiJ9YAqto (ZDF documentary)

Holland, M. (2020, February). #Cryptoleaks: CIA und BND steckten jahrzehntelang hinter Verschlüsselungsfirma. *Heise Online.* https://www.heise.de/newsticker/meldung/Cryptoleaks-CIA-und-BND-steckten-jahrzehntelang-hinter-Verschluesselungsfirma-4658033.html

Viola Amherd trennt sich von Geheimdienstchef Gaudin (2021, May 12). *SRF*. https://www.srf.ch/news/schweiz/nach-meinungsverschiedenheiten-viola-amherd-trennt-sich-von-geheimdienstchef-gaudin

References

Aldrich, Richard J., & Müller, Peter F., & Ridd, David, &Schmidt-Eenboom, Erich (2020, June 4). Operation Rubicon: sixty years of German-American success in signals intelligence. *Intelligence and National Security, 35(5), 1–5.* https://doi.org/10.1080/02684527.2020.1774849

Reuvers, P., & Simons, M. 2020. Operation RUBICON. Cryptomusuem.com. https://www.cryptomuseum.com/intel/cia/rubicon.htm

Wayne, M. (1998). Crypto AG: The NSA's Trojan Whore. *CAQ, 36-42. https://covertactionmagazine.com/wp-content/uploads/2020/01/CAQ63-1997-4.pdf*

Sarah Mainwaring (2020, June 4). Division D: Operation Rubicon and the CIA's secret SIGINT empire. *Intelligence and National Security, 35(5), 623-640. https://*doi.org/10.1080/02684527.2020.1774854