Shadowing 'the exceptional' behind the 'ordinary': mapping a network of intelligence laundering

Vanessa Ugolini & M. L. R. Smith

*Correspondence to: M. L. R. Smith. Email: Mike.smith@kcl.ac.uk

Abstract

Under the imperative of 'prevention', the process of information production for investigatory purposes forms a crossover between intelligence gathering and law enforcement. Digital surveillance programmes collect personal data prior to any probable cause of suspicion, whereas law enforcement activities are concerned with collecting evidence of crimes after the event. When future looking preventative approaches to the prosecution of crimes are forced into the linear, temporal narrative by which criminal investigations unfold, a tension emerges. The article demonstrates the ultimate incompatibility between 'out of the ordinary' intelligence activities and 'ordinary' criminal investigations by unearthing the procedural character behind evidence laundering.

The risk posed by individuals and groups deemed to be a threat to society demand investigatory speed and efficiency in order to interdict the dangers they pose. Dismantling organizations and networks, and detecting crimes ahead of their materialization often requires a multi-level approach. Cooperation and information sharing among different agencies is the cornerstone of intelligence-led policing. What the United States Drug Enforcement Agency (DEA) describes as 'investigative intelligence', for example, aims explicitly to collect information on both active and potential targets with the ultimate goal of bringing prosecutions. In the DEA's own words: 'Underpinning this era of intelligence is a new philosophy that states that intelligence drives enforcement'.[1]

Through the Special Operations Division (SOD), DEA intelligence analysis supports federal, state and local law enforcement officials in compiling investigative reports.[2] The work of the SOD in collating, analysing and disseminating intelligence derived from multi-agency collection efforts enables criminal cases to be enacted.[3] Armed with legal investigative authority, the SOD is able to build and pursue leads. 'Packed intelligence' derived from the surveillance efforts of intelligence agencies, such as the National Security Agency (NSA), is then passed on to local field offices for real-time enforcement investigations.

It is within the intersection of the 'guilds of professionals'[4] of policing and intelligence that the gathering and sharing of data under the imperative of 'crime prevention' takes place.[5] These professional guilds, such as police forces, intelligence agencies and private contractors, utilize methods that between them extract evidence and turn it into 'actionable data'.[6] Therefore, the efforts of the intelligence community and of law enforcement interconnect at the level of information production leading to prosecutorial cases. The complexity of the interactions among official, public, private and clandestine actors, informed as they are by distinct dynamics and processes, however, makes it exceedingly difficult to map those connections on paper.

Framing the debate

The analysis that unfolds below attempts to clarify and make sense of the complexities. While the assessment inevitably deals with the technical and legal debates, the broader relevance of this analysis both for scholars of intelligence, policy makers, intelligence and law enforcement officials should be highlighted. Given the interlinked nature of many contemporary threats, ranging from violent non-state actors, to organized crime as well as cybercrime, it is increasingly likely, if not the case already, that the building of evidence for prosecutions will require cross-border collaboration among national agencies. Almost certainly this effort, in part, necessitates the exchange of sensitive data based on the principle of the pre-emptive acquisition of intelligence data.

As data are exchanged among security agencies, they travel through different sites of security authority. Their substance is therefore constantly shaped and re-shaped according to the different purposes for which they are appropriated. In a growing number of criminal cases, law enforcement agencies require access to data, in particular digital data, stored by service providers in third countries. Digital data in the age of the Internet is perhaps the ultimate transnational phenomenon of our times. Accordingly, the idea that data extraction for investigatory and law enforcement purposes is necessarily something that can be reliant solely on domestic repositories of information is something that cannot be assumed. The transnational communication of data in the cyber sphere occurs as a matter of routine with such high frequency that already puts the control of information flows well beyond the jurisprudence of national oversight bodies. It should be evident, therefore, that the implications of the preventive acquisition of data in the digital age touches on crucial debates within the realm of intelligence oversight, with attendant consequences for ethical considerations, along with questions about the potential of such methods to further politicize intelligence gathering, as the subsequent analysis will make clear.[7]

Of particular relevance in this respect, when contemplating measures that can regulate the use of cross border digital data for domestic prosecutions, questions of territorial jurisdiction emerge. Here, issues of oversight loom large. Although the empirical analysis in this article focuses on the case of the United States, the fundamental concerns this analysis raises are more universal in nature. In fact, the oversight problem is even more prominent in the case of the European Union (EU), for example, where cooperation among law enforcement, judicial authorities, and service providers (most of which are located in the U.S.) occurs primarily on a voluntary basis premised on mutual support among friendly nations. For the EU, the problem of oversight is exacerbated by the absence of an EU-wide approach for regulating requests for electronic evidence from service providers headquartered in another EU member state, or where the location of data storage resides in a third country. Such fragmentation in the legal framework relative to the collection and transfer of evidence between EU states constitutes a significant challenge for enforcing jurisdiction in the cyberspace.

Moving to the specific intent of this article, the aim is twofold: first, to uncover the channels through which classified evidence derived from intelligence collection efforts is re-purposed for orthodox criminal investigations; and second, to evaluate the logic of prediction behind information sharing by revealing the network of clients and suppliers that are committed to support the information flow among federal and security agencies. Unearthing the procedural character behind evidence laundering reveals the tension, and ultimately the incompatibility, between ‘out of the ordinary’ intelligence activities and ‘ordinary’ criminal investigations.

Whereas the former aims to be proactive in the collection of intelligence material, the latter is inherently reactive because it responds to a committed criminal act.

Basing the analysis primarily on the case of the United States, this paper scrutinizes judicial decisions, court rulings, briefs from federal and state criminal cases as well as general court records where classified information has been 'walled off' and funnelled into routine – or 'ordinary' – criminal investigations. In particular, it examines how the two-fold evidentiary trail has been shaped through the fusion of the overt process of criminal investigations and the covert process of information gathering through clandestine – and sometimes warrantless – surveillance and the use of personal data.[8] Before moving to the analysis, the paper outlines how the practice has emerged in the United States against the backdrop of the post-9/11 intelligence setting. The discussion then proceeds by breaking down the stages by which the parallel investigatory construction unfolds.

Background and approach

The practice of dual-track evidence gathering was disclosed in 2013 by *Reuters* that reported that the DEA was funnelling information from intelligence (domestic/overseas) intercepts, most notably from a vast database of telephone records, known as 'Hemisphere'.[9] The 'packed' information was then handed over to local law enforcement officials with the intention of re-constructing the investigatory trail in order for criminal cases to be opened.[10] In the same year, the *New York Times* reported on a similar theme revealing the use of large-scale data for law enforcement, rather than for national security.[11] The report was based largely on the de-classified, but redacted, 'Synopsys of Hemisphere' document released in the form of a Power Point presentation and marked as 'Law Enforcement Sensitive'.[12]

Although the topic has been subject to extensive media coverage, this has not been mirrored in the academic domain. While the role of Big Data technologies in the practices of security agencies has received scrutiny from transversal disciplines, such as critical security studies and Science and Technology Studies, the parallel construction of the investigatory trail has yet to be bridged to existing debates concerning digital surveillance and prevention strategies. The reason for this arises possibly because of the difficulties of evaluating the technical aspects of the practice together with the legal and ethical issues they engender. To fill the gap, this paper analyzes the functioning of parallel construction as a channel through which intelligence activities and law enforcement investigations are reconciled.

In order to undertake the analysis, three strands of literature are engaged. The first strand encompasses court rulings and government documents obtained by public disclosure through Freedom of Information Act (FOIA) and California Public Records Act (CPRA) requests.[13] The Electronic Frontier Foundation (EFF) and the Electronic Privacy Information Centre (EPIC) store material gathered under these auspices. As part of their 'Transparency Project',[14] both EFF and EPIC have made several appeals for public records concerning the acquisition of sensitive information by law enforcement authorities from telecommunications providers outside the standard judicial process.[15] Two requests in particular have been submitted to seek records related to the 'Hemisphere Program', one to the DEA[16] and one to the Los Angeles Regional Criminal Information Clearing House (LACLEAR).[17] The EFF's FOIA request for 'expedited processing',[18] for instance, pertains to information for which 'there is an urgency to inform the public about actual/alleged federal government activity'.[19] Given that both requests returned only heavily redacted records, the EFF filed two litigations against the US Department of Justice and the California Attorney General's office to force

law enforcement to release the information.[20] On the same grounds, EPIC prevailed in a FOIA lawsuit following the failure of the DEA to conduct Privacy Impact Assessments (PIAs) required by law.[21] The list of records that the government is withholding from both EFF and EPIC is nevertheless arbitrary. An attachment to the Hemisphere Power Point Presentation, released by the investigatory news site *Muckrock*, revealed that there are only 161 pages in common to both lawsuits.[22] However, the redacted pages have been withheld on the basis that their disclosure could interfere with ongoing law enforcement investigations.

Beyond this primary material, the paper relies on a second strand of literature to shed light on the substance of the data gathered. In particular, drawing on studies on the functioning of link analysis aims to compensate for the gap in the technical knowledge relative to data-mining techniques and the algorithmic process behind the Hemisphere programme. Further, to evaluate the tensions between clandestine intelligence gathering and routine criminal investigations, this paper engages a third strand of literature encompassing several statutory regulations, in particular the US PATRIOT Act, the Foreign Intelligence Surveillance Act (FISA) as well as the Fourth, Fifth and Sixth Amendments of the US Constitution. Analysing the formal legal framework enables an assessment of the implications that the parallel construction practice engenders on the traditionally linear criminal justice process, most notably on the right to a fair trial and the presumption of innocence.

Sharing information transversally

The DEA lesson plan titled 'Handling Sensitive Information', and disclosed by the journalist C.J. Ciaramella, discusses the post-9/11 national consensus concerning information sharing.[23] The document outlines the advantages of pairing information received in the form of tip-offs from intelligence agencies and of transferring that information to law enforcement bodies for the purposes of prosecution. Against this backdrop, it is possible to outline the emergence of the so-called fusion concept. Prior to the events of 9/11, the intelligence sharing process was highly constrained. Intelligence agencies were not obliged to disclose information to other intelligence agencies (horizontally), neither were they committed to share intelligence with law enforcement authorities, such as the FBI (vertically).[24] Post-9/11, however, federal, state and local authorities were directed to cooperate so as to increase preparedness for domestic terrorist attacks, major disasters, and other emergencies.[25] Accordingly, the fusion concept requires a multi-agency collaborative effort in the provision of expertise, resources and information (transversally).[26]

The goal of transversal information sharing is to maximize the ability to detect, apprehend and ultimately prevent criminal and terrorist activities before they materialize. In this sense, fusion centres function as 'puzzle builders',[27] whereby the pieces received from each investigative agency are plugged in to build the larger picture envisioned in the phrase 'connecting the dots'. The key to operational success is founded upon a coordinated effort to anticipate, identify and ultimately prevent criminal activity.[28] Fusion centres thus function as aggregators of information, that is, central hubs, responsible for referring tips and developing leads aimed at safeguarding homeland security and preventing criminal activity. This rationale is clearly stated within NCRIC records submitted to EFF on 28 December 2013 following the FOIA lawsuit. The cover sheet to the NCRIC document reads as follows: 'Fusing information, talent, training for a safer society', and continues: 'Information needed by fusion centers to prevent organized crime, terrorist and street gang-related criminal activity has to be collected from personnel trained in information collection, informant development and mainly information sharing'.[29] Operational success is therefore based on the

ability to efficiently and securely process and share information across all sectors of law enforcement and the intelligence community.

In 1997 the Northern California High Intensity Drug Trafficking Area (HIDTA) pioneered this model of information sharing and dissemination. The HIDTA programme covers an investigative support centre, a training programme as well as an equipment-lending programme. Instituted as an 'Information Sharing Program', the Northern California Regional Intelligence Center (NCRIC) came to function as the clearing-house for the collection, analysis and dissemination of information.[30] The Center encompassed a network that includes four regional centres established in late 2004 and located in San Francisco, Los Angeles, Sacramento and San Diego. Tips and leads may flow from the intelligence community, police, media, informants as well as private companies and business partners. It is then the responsibility of the NCRIC to collate the data, determining its credibility and assess the underlying threats until a criminal connection is discovered. In this sense, the 'all crimes, all threats, all hazards'[31] approach to law enforcement is based upon a multi-agency effort to enact the prosecution of crime. As stated in a speech delivered by the then President George W. Bush:

> The Department of Homeland Security is working to strengthen cooperation with state and local governments, so we can prevent terrorist attacks and respond effectively … We have done so by helping state and local officials to establish intelligence fusion centers in 46 states. These centers allow [locally generated information] to get to our state and local partners.[32]

According to the legal analysis conducted by Hanni Fakhoury on behalf of the Electronic Frontier Foundation, the implementation of unconventional sharing rules after 9/11 allows intelligence agencies to hand over classified information to domestic law enforcement, with no connection to on-going national security investigations.[33] As a result, the deployment of clandestine intelligence surveillance powers in ordinary criminal investigations eliminates the bar to information sharing between law enforcement and intelligence agencies.

The intelligence-led policing model

The evolution of parallel construction has been ground breaking for the development of the 'intelligence-led policing' model, underpinned as it is by the assumption that 'terrorism' – or perhaps more accurately politically motivated sub-state violence – can be intertwined with other crimes. As reported by *Time*, the DEA's activities have been re-framed since 2006 to encompass counter-terrorist efforts along with its traditional role in dismantling drug and narco-trafficking organizations.[34] In support of such efforts, the information funnelled from NSA wiretaps, electronic intercepts as well as from data mining of millions of phone and digital records provide leads vital to DEA operations seeking to connect suspect criminals to politically motivated violent conspiracies. The federal agencies involved in parallel construction form part of a distribution network aimed at disseminating information transversally. This network comprises DEA, SOD, NSA, FBI, Immigration and Customs Enforcement (ICE), the US Department of Homeland Security Investigations, the Internal Revenue Service (IRS) as well as the Bureau of Alcohol Tobacco Firearms and Explosives, among others.[35]

In terms of coordinating and sharing intelligence for law enforcement purposes, the Special Operation Division is the most forward-looking. Focused on investigating cases in which drug trafficking and terrorism crossover, the SOD is at the core of the DEA's efforts.[36]

Indeed, the Division has been nicknamed the 'Dark Side of the DEA'.[37] While it does not feature as an official entity, the SOD has been configured to intersect transversally with the criminal justice system and the intelligence community. As reported in *The Huffington Post*, it encompasses personnel from a number of security agencies, including the FBI, CIA, NSA as well as the US Department of Homeland Security.[38] Therefore, the SOD functions as a multi-agency coordinating body and figures as the principal node of the DEA distribution network. Through its controversial relationship to domestic law enforcement, the SOD is responsible for referring leads to local authorities nationwide in a manner that ensures the origins of those leads are not revealed in formal prosecutorial proceedings. The logic is clearly set out in the manual provided to the agents of the Internal Revenue Service which, states that the purpose of IRS investigations consists of 'protecting the sources and methods', and 'not to withhold evidence'.[39] The manual contains a 350-word entry describing parallel construction and instructing agents of the US Tax Agency to omit any reference to the tips supplied by the SOD among investigative reports and affidavits.[40]

Constructing a channel to funnel intelligence information

Several public reports have revealed that communications data derived from intelligence intercepts, wiretaps and the data mining of private telecommunication companies are being exploited for law enforcement purposes.[41] *TechCrunch* speaks of 'a direct connection between the NSA, and its surveillance efforts, and regular criminal prosecutions in the country'.[42] Nevertheless, while unclassified material can be used as evidence against criminal defendants, classified material, including sources, methodologies and technologies, must be protected from disclosure in courtrooms. The reasoning is purely practical: ensuring that intelligence activities remain effective to the extent that they are covert. The Drug Trafficking Administration Legal Instruction Unit – based in Quantico, Virginia – explicitly devised a Lesson Plan as part of a course targeting entry-level federal intelligence analysts aimed at resolving this law enforcement tension.[43]

Reading more closely, the Lesson Plan comprises eight versions of a training module originally created in 2007 and entitled 'Handling Sensitive Information'. The Plan received formal re-validations in 2008, 2009 and 2012. Each version sets out the core procedures that can accommodate the use of intelligence information in criminal investigations by Law Enforcement Agencies (LEAs). According to the 2012 Lesson Plan, the overall objective is to 'identify legally acceptable methodologies for handling the problem of combining the collection capabilities of the Intelligence Community (IC) with the objectives of LEAs without unduly risking disclosure of sensitive, classified IC information in the open, public trial system'.[44]

The practice of creating a secondary, alternative, investigatory trail stems from this rationale. The issue speaks to the incompatibility between the collection capabilities of the intelligence community and law enforcement investigations. Intelligence agencies collect clandestine, covert information, expecting material and sources to remain undisclosed. Law enforcement, conversely, must be transparent about information, while also being required to introduce such evidence into court as part of a prosecution against a defendant. According to the DEA, the mismatch is reconciled by reverting to the technique known as 'parallel construction'.

The technique has been devised to address the distinct classification levels of sensitive material, which comprise: 'confidential' (damage), 'secret' (serious damage), 'top secret' (exceptionally grave damage).[45] The latter pertains to highly classified information, which

because of its especially sensitive nature, cannot be introduced as evidence into open court. Among the unclassified DEA records, 'shielding' and 'walling off' are two recurrent terms used when referring to the practice. In the training modules scrutinized by *Muckrock*, federal agents are instructed to resort to parallel construction to shape the evidence chain in such a way that neither the prosecution nor the defence are aware of the use of classified information in routine criminal investigations.[46]

Human Rights Watch defines the practices of parallel construction as: 'The efforts by government bodies to conceal the true origin of evidence by creating an alternative explanation for how authorities discovered it'.[47] Several other definitions of parallel construction have been offered both in the press and in classified documents. Combining elements of these definitions, this study defines parallel construction as the secret process of building the legal basis of a case by seeking evidence originally obtained through intelligence methods via normal investigative procedures. Thus, while leads are generated through secret programmes of clandestine surveillance and then passed on to law enforcement to launch criminal investigations, a parallel story is fashioned in order to obscure the derivation of the original lead.

The procedural character of parallel construction can be broken down as follows:

1. It starts off with the collection of data by intelligence agencies, such as the NSA, by mining datasets of private telecommunication companies containing millions of calls and digital records.
2. Tips are then transformed into 'actionable intelligence' through data mining techniques and link analysis in order to connect otherwise disparate clues about the calling patterns of persons of interest.
3. Once raw data have been transformed into actionable information, tips are funnelled to federal or other local law enforcement agencies.
4. Law enforcement agencies 'launder' the intelligence obtained through clandestine surveillance by submitting a subpoena for persons of interest, authorizing the initiation of an investigation.

As a result of working backwards the investigative trail stemming from the original tip, a two-fold evidence chain is established. The underlying strata is made up of material concerning classified information obtained through high-tech data mining methods, while the overt trail consists of an independent, legal body of evidence, constructed by going through the motions of re-discovering incriminatory evidence through less controversial methods. In such a way, the classified source of the investigation – that is, the domestic/foreign email intercept, wiretap, or mined Call Detail Records (CDR) data – is effectively covered up.

'Shielding', 'walling off' and 'covering up': 'how to' build parallel construction

The DEA training material sets out various tools used to re-create the evidence chain without exposing intelligence sources and methods to the public trial system. An annex to the DEA Lesson Plan, titled 'Traffic Stops – Legal Issues', illustrates the widespread technique known as 'whisper', 'wall' or 'wall off' stops.[48] The technique follows a simple logic: local law enforcement officials may receive a tip-off from an intelligence agency about a vehicle containing drugs based on the cell phone surveillance of a target. The tip is usually passed on in the form of 'Be On the Lookout Orders' (BOLOs).[49] For instance, an intelligence agency

contacts a local law enforcement official with the instruction to 'look out for a white car, at such intersection, at a specific time'.[50] The officer conducting the 'random stop' usually initiates the search in a way as to look like a routine traffic stop or a minor traffic infraction. If drugs or illegal weapons are found the driver is arrested. As the trial phase follows, local police officials are bound by a statutory order to protect the confidentiality of the source, enabling them to declare that the investigation began with the routine traffic stop. This legal provision is clearly stated in the material gathered on the Hemisphere Project instructing officials to 'never mention or refer to Hemisphere in official reports or court documents'.[51] Thus, by working the evidentiary chain backwards, the received intelligence is, in effect, 'laundered' while a new investigative trail that will not lead back to the origin of the source is thereby generated. On this basis, parallel construction can be envisioned as a 'shield' separating the two parallel investigatory trails, stemming nonetheless from the same intelligence source.

Project 'hemisphere': the super-search engine

According to *Wired*, law enforcement officials have managed to secure routine access to a database code-named 'DICE', which stores details of every call, text message and Skype communication passing through the AT&T network.[52] The first references to DICE surfaced in 2013 after the *New York Times* revealed the existence of 'the largest secret telephone records surveillance program', called 'Hemisphere''.[53] According to the 'Synopsys of Hemisphere', the project is coordinated from the LACLEAR and is funded by the Office of National Drug Control Policy (ONDCP) and the DEA in cooperation with AT&T.[54] Given the vastness of the AT&T network, which reportedly owns three quarters of US phone systems, including landline switches and cell-phone towers, law enforcement agencies are able to retrieve phone records on any call passing through the AT&T network, including calls routed through any AT&T switch.[55] With approximately four billion records added daily, the Hemisphere database tends, unsurprisingly, to attract sensationalized headlines. Touted by police officers as a 'Super Search Engine' and 'Google on Steroids',[56] the potential of its software record system to reach into numerous stove-piped databases enables the extraction of Call Data Records on a near-real time basis. Through Hemisphere, federal, local and state police officials are provided with access to an enormous telecom database containing trillions of domestic and international electronic call records dating back to 1987.[57] From LACLEAR's records, one federal agent stated: 'The goal is to see if the [Hemisphere] system will help us "work smarter" and increase intelligence-driven investigations'.[58]

Issuing subpoenas

Depending on the records sought, CDR data is retrievable from Hemisphere and returned via email to law enforcement agencies within as little as one hour of the submission of a subpoena.[59] An administrative or Grand Jury subpoena consists of a declaration that information to be retrieved among the billions of phone records retained by AT&T *'could be relevant'* to an investigation.[60] Unlike a search warrant, which requires state officials to submit a statement demonstrating 'probable cause' that any records sought are *'relevant'* to a preliminary investigation,[61] the order for Hemisphere is issued directly by law enforcement agencies, thereby enabling circumvention of court oversight. The requested CDRs are then released in the form of an official subpoena response.

As explained in the responsive documents released to both EFF and EPIC,[62] data obtained through Hemisphere cannot be introduced as evidence in courtrooms. Consequently, the tip-

off funnelled to a local law enforcement agency by a classified intelligence source is 'walled off'. The same information is then sought out again in a way that can legitimately be used as evidence in a courtroom. The Power Point slides outlining the Hemisphere Project refer to the practice as 'parallel subpoenaing'[63]: for every result produced by accessing Hemisphere call records, the government issues subpoenas to re-obtain a complete set of CDRs from the official carrier. Nevertheless, as per the 'non-disclosure agreement',[64] the original subpoena request remains obscured as it is not to be referenced by local police authorities in investigative reports. This way, the records regarding the phone numbers originally identified by Hemisphere can be attributed to the official provider. In other words, leads produced by mining the Hemisphere database are provided to the DEA by AT&T and then 'laundered' by investigators through routine police work – that is, by obtaining a court order for a domestic wiretap. As a result, only the second, re-constructed evidence is employed as part of a prosecution.

Hemisphere's submission request process

In response to the FOIA requests issued by the Electronic Privacy Information Center,[65] the DEA released information[66] pertaining to the Hemisphere Programme outlining the 'Hemisphere Request Process' (Figure 1).[67] The responding documents included a facsimile of the 'Hemisphere Project Request Form' (Figure 2), also found in the records obtained by the Electronic Frontier Foundation from LACLEAR.[68] Most pages were redacted in order to hide the names of the police and law enforcement agencies involved in the process. A section titled 'Introduction and Request Tutorial' outlines, step-by-step, how to submit a request for a phone number of interest; how to prepare a subpoena; and, lastly, how to interpret the results produced by Hemisphere (see Figure 3).

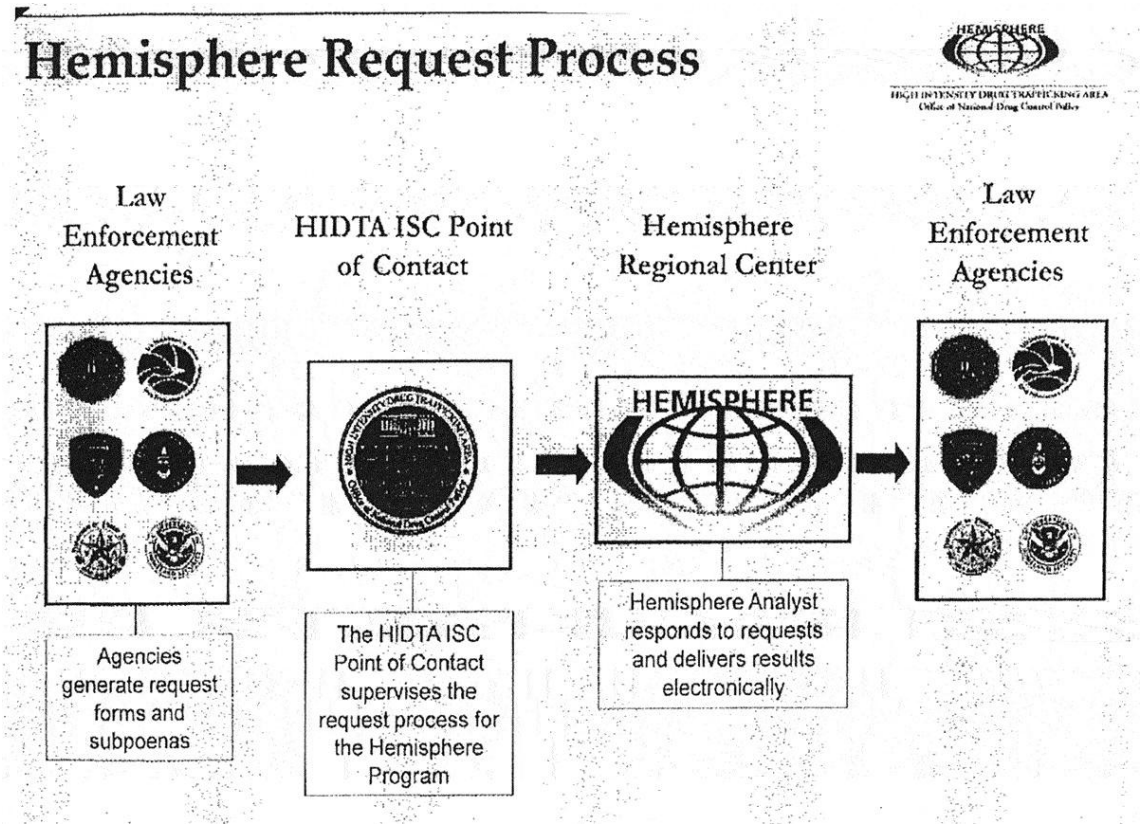

Figure 1. Hemisphere Request Process.[134]

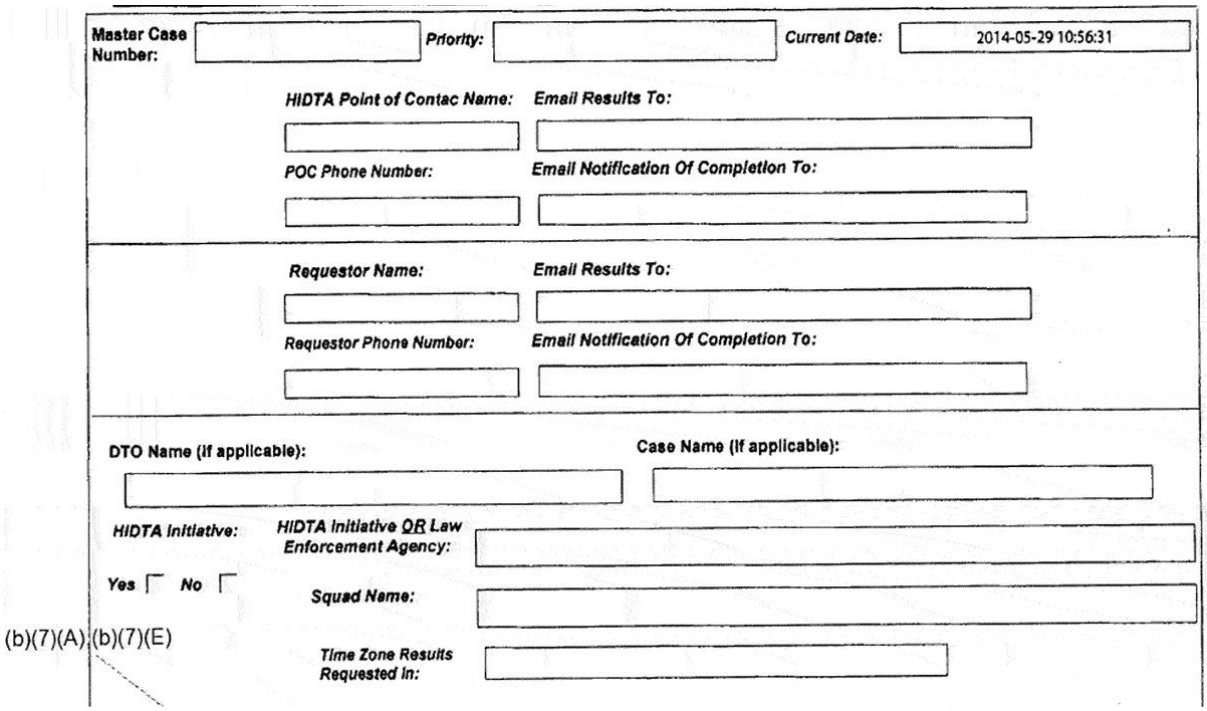

Figure 2. Hemisphere Project Request Form.[135]

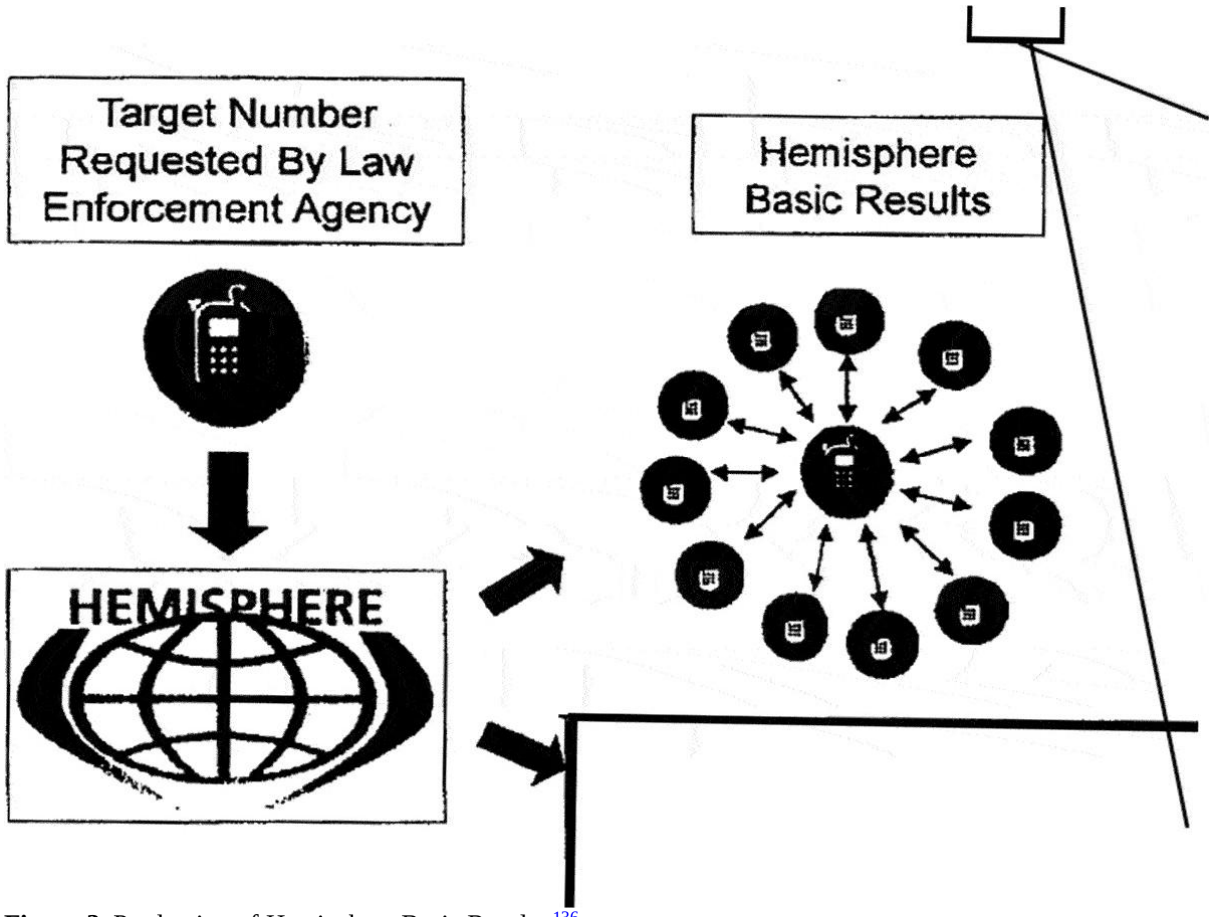

Figure 3. Production of Hemisphere Basic Results.[136]

The tutorial starts by re-stating the non-disclosure clause, that: 'All Hemisphere requesters must protect the Hemisphere program'.[69] The document further specifies the fields to be compiled and returned with a full record of the subpoenaed number(s). To generate a subpoena, law enforcement agencies must fill in the 'Hemisphere Request Form' with a valid email and telephone number (see Figure 2). All requests must then go through a designated Point of Contact belonging to a HIDTA Investigative Support Center (ISC), embedding analysts that have been trained by a certified Hemisphere instructor on the sensitive nature of the programme.

Further, to assign the appropriate level of action to each request, the 'Priority' section has to specify the 'level of urgency'. Multiple data ranges for when the phone was active can be included. The results are then split according to the specified ranges before being returned to the respective requesting law enforcement agency. Once the records have been retrieved, AT&T analysts assist law enforcement clients in the interpretation of phone records. For routine requests, the average return time of the subpoenaed CDR data is 2–5 days. Results are then delivered in electronic format.[70] According to *The Daily Beast*, Hemisphere is now in operation in 28 of the intelligence fusion centers that figure as part of a wider network embedding AT&T employees in government drugs investigation units.[71]

The unclassified 'Synopsis of Hemisphere'[72] further details the kind of information produced by querying the Hemisphere database for the subpoenaed numbers. According to the slides released, CDR data, such as the time, date and length of calls, can be made available from as little as two hours after a call is placed.[73] Among Hemisphere's special features is the capacity to detect dropped phones through an algorithm that analyzes calling patterns to find new numbers as well as additional phones the target is using. Advanced results of a query can produce two levels of call detail records by examining direct contacts for the original number of interest.[74] In addition, it can capture cellular traffic for international numbers that place calls through, or roam on, the AT&T network. Furthermore, by capturing local, long distance, international phone traffic, Hemisphere can aid investigators in tracking targets, while detecting the precise area and time of the call. Initially subscriber information was excluded from its special features, but in 2012 Hemisphere began also to provide that information for AT&T phones.[75] Overall, data collected via Hemisphere can thus provide a variety of different leads for an array of investigations.

'Opacity, invisibility and secrecy': link analysis and data mining

In 2007 when the first references to the Hemisphere programme began to surface, AT&T had already been accused of handing the Federal Bureau of Investigation (FBI) telephone records retrieved by mining its own database.[76] Subsequent disclosures revealed that the FBI had been requesting 'Communities of Interest' records for some customers of the AT&T telecommunication network without a warrant.[77] The *New York Times* refers to secret demands for records as 'National Security Letters'.[78] By submitting such requests, law enforcement agencies could obtain data on designated targets as well as on their 'Community of Interest', that is to say, a network of people that the target has been in contact with.[79] The scope of such national security letters is broad. By mining the Hemisphere database, law enforcement bodies could retrieve information about who a target called most frequently, for how long, at what time of the day, which geographic regions were called as well as tracing fluctuations in phone activity.

The term ‘Community of Interest’ – or COI – made its first appearance in a conference paper published by AT&T in 2001.[80] The manual illustrates through practical examples and readable graphs the ‘Guilt by Association’ procedure, used to detect fraudulent behaviour among cellular traffic by clustering nodes.[81] The label ‘Guilt by Association’ derives from the reasoning implying that criminal behaviour forms an affinity group that can be mapped out by plotting a connectivity network.

Hancock: an ad-hoc programming language to perform traffic analysis

To analyze ‘Community of Interest’ data, such as long-distance calls, and performing link analysis on the material gathered through Hemisphere, AT&T relies on the implementation of a C-based domain-specific programming language called ‘Hancock’.[82] Developed in the 1990s by AT&T researchers, the Hancock C-variant was intended originally to extract information for marketing strategies and to optimise its network through new service offerings.[83] According to *Wired*, in 2001, the software was transformed into a security tool employed to mine gigabytes of telephone and Internet records for surveillance purposes.[84]

Through Hancock, analysts perform record linkage analysis in the attempt to identify replacement, dropped or additional phones. The ability of Hancock’s algorithms to run against streams of data enables the linking of otherwise unstructured, disparate clues and thus to build a complete picture of a target number’s phone activity. When new accounts get activated on the AT&T network, high-tech data mining techniques are used to associate an abandoned telephone number with a replacement phone, based on the examination of calling patterns.

Given that Hemisphere contains a huge volume of unstructured records, the establishment of associations among data points demands speed and performativity. As a result, the Hancock code has been designed to facilitate signature computations in such a way that the average time for retrieving and deriving a dataset takes only about one second.[85] Specifically, the analysis of so-called ‘transactional data streams’ consists of a sequence of call records that log interactions between pairs of entities over time.[86] Hancock is therefore qualitatively different from traditional data mining applications, which detect patterns among static databases. As further detailed in the 2004 paper published in *ACM Transactions on Programming Languages and Systems*, Hancock’s algorithms can sift through long distance calls, IP addresses and Internet traffic as they flow instantaneously into the data warehouse.[87] Its ability to capture fluid data enables the location of mobile phone customers to be tracked, as the original signal moves from one cell site to another. As a result, Hancock can re-create a map of a person’s movements by recording which cell phone towers the number of interest had pinged throughout the day.

Mapping ‘Communities of Interest’

The fields relevant to draw up a ‘Community of Interest’ include the ‘total duration of calls’ as well as the ‘number of calls’ made.[88] As explicated in the 2001 research paper, the aggregation function logs such measurable entities on a time-varying graph featuring nodes as transactors, and edges as interactions between pairs of nodes.[89] The graph is dynamic since both nodes and edges can appear and disappear throughout time. A move away from clusters of data, detected by measuring the distance among nodes, is indicative of dissonance, dissimilarity and oddity. Indeed, the underlying reasoning equates the non-membership of a data point in any given cluster to an ‘anomaly’.[90] For instance, Figure 4 exemplifies a ‘Guilt

by Association Plot' where, for any node surrounding a suspect phone number labelled as fraudulent – XXX8667665 – new accounts belonging to the same COI get immediately deactivated upon suspicion of fraudulent behaviour.[91]

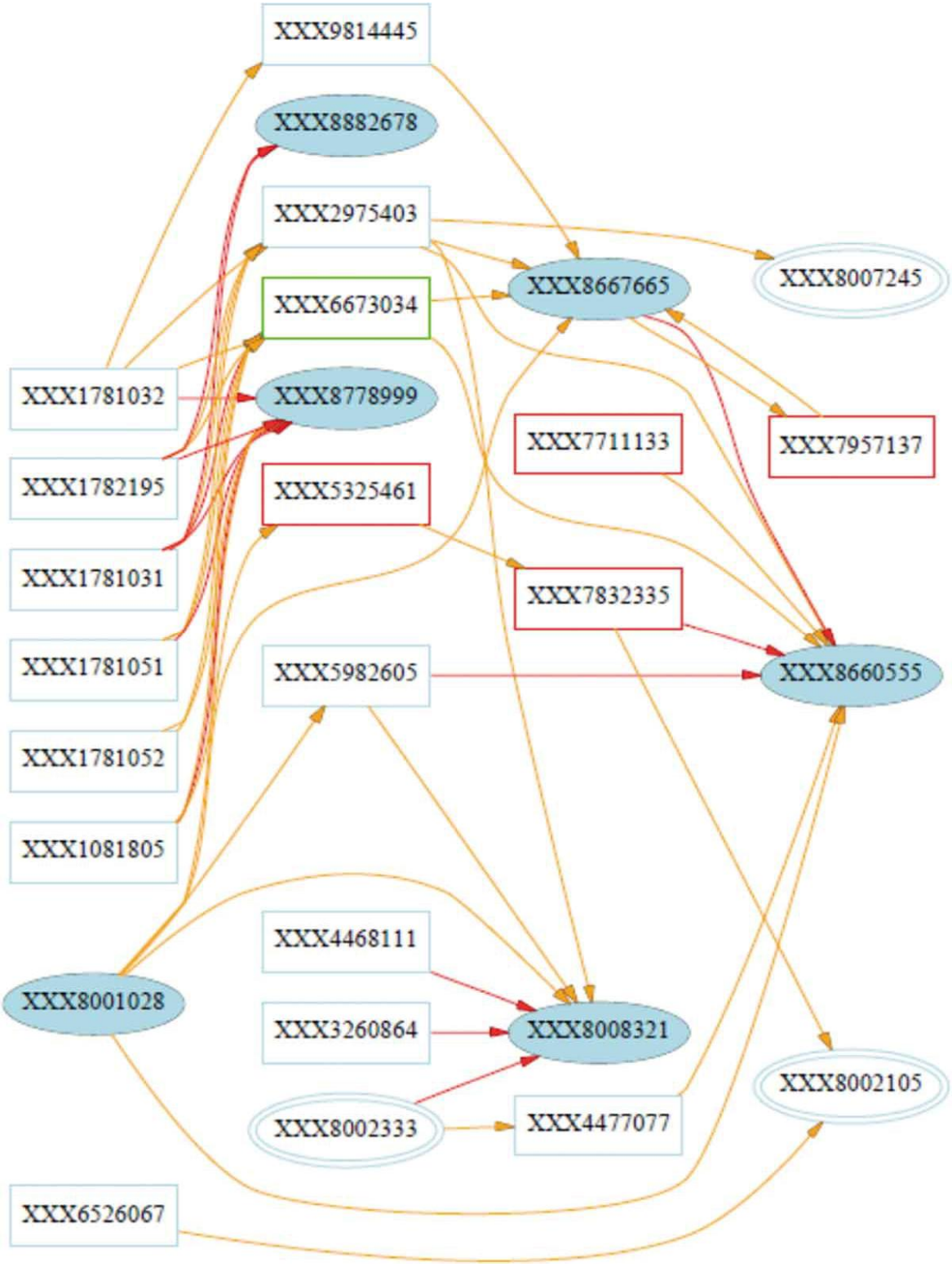

Figure 4. Exemplifying a Guilt by Association plot

Source: Cortes, Pregibon and Volinsky, 'Communities of Interest,' 8 (Reproduced with permission from Springer Nature).

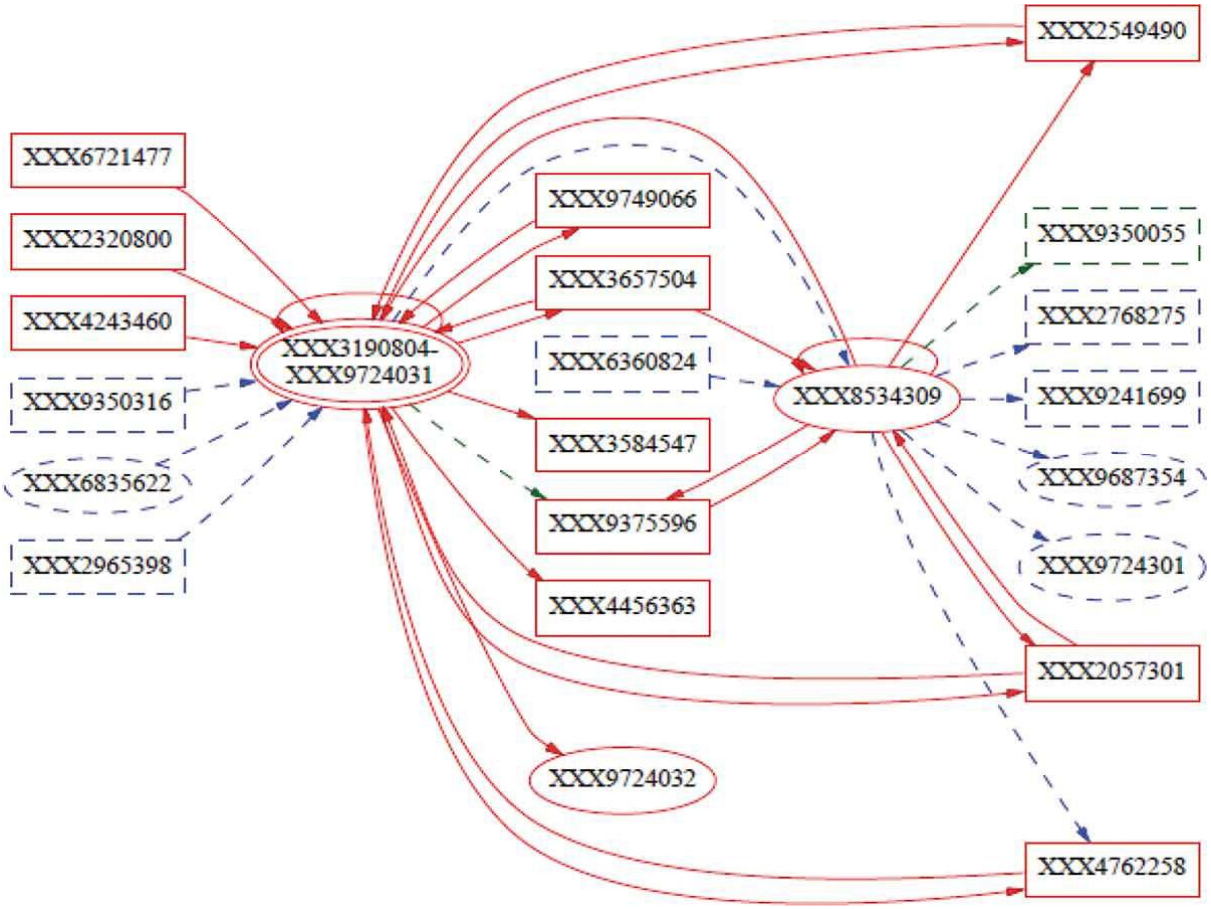

Figure 5. Visualization of linking accounts by their COI

Source: Cortes, Pregibon and Volinsky, 'Communities of Interest,' 10 (Reproduced with permission from Springer Nature).

The distance between two or more COIs depends on some inherent features such as the 'quantity' of nodes, measured by calculating the number of COIs consisting of overlapping nodes; and their 'quality', that is, those nodes which are informative and under consideration for a match.[92] The probability that an account is 'fraudulent' correlates to the number of suspect nodes within the COI. Therefore, the score ranks high for those COIs with strong links to the node of interest. It follows that 'riskiness' is inferred on the basis of the connectivity of a node to fraudulent/legitimate nodes, determined by plotting a 'Guilt by Association' network. This procedure permits the labelling of nodes as suspect or legitimate as a result of their disposition in the virtual space, and where the decision tree of algorithms generates a score by calculating the closeness/distance between node pairs. In practical terms, for any COIs appearing on the plot, analysts can determine whether a newly activated account belongs to a recently disconnected or dropped number, with the same individual behind it.

The pattern-seeking process underlying the 'Guilt by Association' procedure reveals the technical aspect of the intelligence-led policing model. The performance of traffic analysis, imported from computer science into the realm of predictive policing, enables the identification of patterns and characteristics that raise suspicion ahead of the materialization of a criminal act. Framed around the notion of 'predictive analytics',[93] the capacity to search, aggregate and cross-reference large datasets is valued by law enforcement and intelligence

agencies since it is central to the formation of predictions.[94] In order to 'connect the dots' among phone records, intelligence-led policing aims to deploy the latest mathematical and computing technologies. In particular, in the determination of the phone records to subpoena, law enforcement agencies employ algorithms for the identification of patterns, characteristics, trends and anomalies among datasets, without having *a priori* knowledge of the substance of the data.[95]

To become intelligible and actionable, information is first gathered and organized through a 'visualization network' in the establishment of associations among data streams.[96] Persons of interest are then identified algorithmically through a systemic exercise of data matching (see Figure 5). By mapping a network of similarities, algorithms eventually learn what is topologically normal, while counting any discrepancy in the same neighbourhood as an 'anomaly'.[97] The inherent difficulty of comprehending such complex algorithms such as 'Hancock' to all except computer coding experts, enables a degree of concealment, intentional or otherwise. In turn, the ability to exercise judicial oversight over their use by security analysts is impaired.

Accordingly, the secrecy surrounding the Hemisphere programme coupled with the absence of up-to-date legal standards regulating the employment of high-tech data mining methods in the context of criminal investigations raises concerns with regard to the permissible limits of government surveillance. In the words of Marc Rotenberg, President of the Electronic Privacy Information Center: 'Agents could be reviewing call records of people who have done nothing wrong'.[98] Through the partnership between AT&T and the DEA, law enforcement authorities are effectively empowered to create networks of conspiracy among suspected criminals and violent subversive threats alike that can ensnare individuals who may not have any connections to criminal activities. The willingness of federal agencies to insulate the practice from public scrutiny, and even from prosecutors and judges, reveals that parallel construction really is 'intelligence laundering'.

Parallel construction versus the criminal justice system

To balance the interest of the state in conducting a thorough search in the name of national security vis-à-vis individual privacy interests, existing Fourth, Fifth and Sixth Amendment principles have been applied. More specifically, the Foreign Intelligence Surveillance Act sets out the regulations guiding the enactment of a search. In *Katz v. Unites States*, the Supreme Court declared that a 'search' occurs where 'subjective expectations of privacy are violated under circumstances that society acknowledges as objectively reasonable'.[99] To initiate the search, authorities must therefore be in possession of an allegation indicating the existence of a criminal activity or threat to national security. Consequently, the demonstration of 'probable cause' must be laid out *prior to* an investigation. The rationale behind FISA is in fact to *first* identify the target and *then* to obtain information on the committed wrongdoing in order to begin its prosecution. Nevertheless, where intelligence collection efforts and law enforcement investigations collide in the proactive aggregation of data, a 'search' occurs against the backdrop of a future-leaning approach to the prosecution of crimes.

Traditionally, law enforcement agencies aim to investigate and prosecute violations of US law by seeking evidence on *a posteriori* basis, namely, *after* a criminal act has been committed. The wrongdoing belongs to the past, while the prosecution of such an act unfolds linearly from the moment of its occurrence, to the final moment by which the criminal is convicted. Conversely, within the intelligence-led policing framework founded on the pre-

emption principle, individuals are caught in a system that subverts the traditionally linear criminal process, based on the issuance of penalties upon completion of a criminal act. In this regard, the following sections assess the off-setting costs that the unfolding of parallel construction within the traditionally linear criminal justice system engenders at the level of civil and privacy rights.

By creating a parallel, 'alternative', story for how an investigation has been launched, a secondary evidence-chain is contrived to 'wall off' the decontamination of information gained clandestinely. Nevertheless, the two-fold investigatory trail stems from the same point of origin, namely, the 'Fruit of the Poisonous Tree'.[100] Legal justifications for the recourse to parallel construction are grounded in interpretations by the US government of cases where such evidence has been introduced. According Human Rights Watch, the only exception to the 'Fruit of the Poisonous Tree' doctrine concerns material gathered through 'a later and lawful seizure – *independent* of the earlier, tainted [unlawful] one'.[101] To facilitate the incorporation of such 'poisonous' evidence, a number of statutory regulations have been called upon. A policy memorandum issued by the Justice Department states that 'any confidential communication to/from or about a citizen acquired under Section 702 of FISA, *Clapper v. Amnesty International USA*,[102] is not to be introduced as evidence against that person in any criminal proceeding'.[103] Therefore, in order to facilitate the incorporation of classified material during trials, the DEA has designed policies that accommodate the treatment of confidential sources for law enforcement investigations.

Instances of these policies are included in the DEA 2007 Lesson Plan, with the objective to articulate procedures that permit the protection of intelligence collection efforts from disclosure in criminal trials. The 'Classified Information Procedures Act' (CIPA) constitutes one of these instances. Enacted in 1980, CIPA relies on 'Federal Rules of Evidence' (FRE) that govern 'relevancy' and 'materiality' of admissible material. Its function is to establish procedures 'to harmonize a defendant's right to obtain and present exculpatory material upon his trial and the government's right to protect classified material in the national interest'.[104] In circumstances where classified information is involved, the CIPA system is meant to be a balancing act between the defence, which may go too far in trying to introduce classified information that is exculpatory, and the prosecution, which may go too far in trying to protect classified evidence. When evaluating the admissibility of classified information – that may or may not be evidence by its own nature and in accordance with the FRE – relevance and materiality are determined as if the information was not classified. In order to evaluate the material, the court first makes use of the FRE existing standards, then focuses on the type of relevant information that is useful to the defence. In particular, FRE 401 defines 'relevancy' as 'evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence',[105] while, 'materiality' concerns 'information that is necessary to the determination of an issue'.[106] The latter concept entails specifically that once evidence becomes material to a criminal case, a judge would not be able to exclude it to the defence. Accordingly, only if the proposed evidence is relevant and material to the defence, the government must disclose it. In addition, FRE 403 permits the exclusion of relevant evidence on the grounds of 'prejudice, confusion or waste of time'.

For classified information that may be admissible according to the evidentiary rules, the Act permits the review of such information during the pre-trial phase, that is, '*ex parte, in camera*'.[107] Under the CIPA, the power to establish which information should be introduced as evidence during the discovery process, and which should be protected from disclosure lies

ultimately with the judge. A judge can issue a protective order to preserve sensitive information from being disclosed. In this regard, case law holds that the judge is permitted to 'deny, restrict or defer discovery or inspection'[108] of classified information that is not exculpatory and is helpful to the defendant but not essential to the defence under the Federal Rule of Criminal Procedure (FRCP) 16(d)(1) (Regulating Discovery – Protective and Modifying Orders).[109] In cases where classified information related to the defendant is involved, and where, neither the prosecution team nor the defence team is aware of its presence, a separate team of prosecutors, referred to as 'Taint Review Team', is responsible for handling the litigation along with discovery issues.[110] In this circumstance, the appointed team intervenes preliminarily, by consulting a judge in the determination of which evidence should be turned over to the defence.

Therefore, the application of the concepts of 'relevancy' and 'materiality' lies with the discretion of the judges who are responsible for weighing the national security interest against the relevance standard. For instance, the DEA Lesson Plan on Handling Sensitive Information includes the case of *Scher v. United States*,[111] where a police agent received a tip-off, which resulted in the surveillance of the target, and ultimately to witness the defendant's illegal behaviour. This case ruled that the source of the agent's information, which caused the defendant to be subjected to surveillance, was unimportant. Similarly, the case of *Scott v. United States* thus stated: 'We have since held that the fact that the officer does not have the state of mind which is hypothecated by the reasons which provide the legal justification for the officer's action does not invalidate the action taken as long as the circumstances, viewed as objectively, justify that action'.[112] To simplify, the source of information leading to an agent's action can be withheld from the defence but remain admissible in court on the basis that the legality of an agent's actions does not depend on what he or she has been told prior to an event but on what the agent saw or overheard when he/she investigated.

According to Human Rights Watch, when defence teams make a motion to discover whether intelligence material has been concealed from a legal proceeding, the prosecution will answer in vague language, lacking affirmation or denial. Even when there is reasonable suspicion to believe that intelligence information lies behind a case the defence will usually be unable to obtain such exculpatory material given the statutory obligation to 'protect intelligence sources and methods'.[113] When parallel construction is set in train, defendants are thereby deprived of the opportunity to question the source of evidence introduced against them and hence to make counter-arguments. Thus, applying constitutional restraints to ensure that the scope and execution of a search for digital evidence fall within the limits of the rights prescribed by existing Fourth, Fifth and Sixth Amendments of the US Constitution is something of a stretch. In order to expose the tensions that arise in the context of criminal trials erected via the parallel construction of the facts, the relevance of each Amendment will be examined below.

The fourth amendment and the protection against 'unreasonable searches'

The 1968 Wiretap Act instituted a statutory obligation for law enforcement to obtain a warrant before intercepting and demanding the content of telephone communications.[114] Subsequently, a 1979 US Supreme Court ruling established that to initiate a 'search', law enforcement authorities must only demonstrate 'probable cause', that is a 'higher level of suspicion as to the presence of criminal activity or a threat to national security'.[115] A search warrant thus requires *prima facie* evidence of wrong doing in order to establish 'probable

cause'. It follows that a search warrant can be an effective investigative tool once it has been determined that there is evidence of a crime, and that further evidence cannot be obtained by other means.

The Fourth Amendment, in this respect, establishes protections against unreasonable searches and seizures by law enforcement authorities. The Amendment is widely understood as protecting what an individual may legitimately expect to keep private against unwarranted intrusion by law enforcement agencies.[116] In particular, the Fourth Amendment concerns:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[117]

Nevertheless, given the impossibility of demonstrating criminal intent before mining depositories of data, the usefulness of the protections offered by the Fourth Amendment in a criminal process erected via parallel construction is negated. The contention of attorney Simon Azar-Farr is that: 'If you could potentially use any information from counterintelligence as part of prosecutions in criminal courts, then you might as well say that we do not have a Fourth Amendment'.[118]

In this regard, the interconnectivity imperative that drives the conduct of link analysis entails that the 'broadest set of metadata' needs to be assembled.[119] More specifically, intelligence analysts compile all the records into a database and then perform a contact chaining process to identify only 'relevant' records. Link analysis is used to trace patterns of communications, which are 'two, three or four steps' removed from the original targeted number.[120] Consequently, by obtaining records that are, at least, 'out to two generations' from the number of interest, police and law enforcement bodies can potentially track down anyone who has been in contact with the number of interest.

Such a procedure, however, does not retroactively add 'relevance' to the vast number of records sought, not related to any specific inquiry. Data gathered must be 'relevant' at the time of collection.[121] Over-reliance on link analysis can therefore bring under scrutiny those individuals whose calling patterns may only be tenuously linked to the target and who may not have any actual connections to criminal activities. For Matt Blaze, professor of Computer and Information Science at the University of Pennsylvania and former AT&T researcher: 'There is always going to be a certain amount of noise' with data collected on people who have no real links to suspicious activity.[122]

Parallel construction can, accordingly, be termed as 'law against law' because, as McCulloch and Pickering observe, it is 'the antithesis of the temporally linear post-crime criminal justice process that commences from the presumption of innocence and progresses through a number of discrete stages involving investigation and evidence collection, charge, trial and, in the case of a guilty verdict, punishment'.[123] In particular, the principle of presumption of innocence functions as a procedural safeguard that operates 'from the very moment a person is charged with a criminal behaviour', that is, *prior to* the beginning of the trial phase.[124] Yet, because parallel construction re-creates the investigatory trail by 'laundering' intelligence, law enforcement agencies are able to observe the innocence principle *ex post facto* in a manner that might give the appearance of observing it, while in practice overriding it through parallel construction.

The Fifth and Sixth Amendments and the procedural due process clause

Both the Fifth and Sixth Amendment allows defendants to challenge the accuracy and veracity of an investigation. The practice of parallel construction, however, raises a concern with respect to the rights of the accused to defend themselves while understanding, questioning and challenging the evidence used against the defendant by the prosecution. According to the Fifth Amendment:

No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a grand jury […] nor shall any person be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law […].[125]

The Sixth Amendment is concerned with the protections to the adversarial process, say, the right of the defence counsel to discover potentially exculpatory information. Hence:

The Sixth Amendment guarantees the rights of the accused to require the prosecution's case to survive the crucible of meaningful adversarial testing … including the right to a public trial without unnecessary delay, the right to a lawyer, the right to an impartial jury, and the right to know who your accusers are and the nature of the charges and evidence against you.[126]

When a case is built upon 'laundered' intelligence, such clauses in the Fifth and Sixth Amendments are rendered obsolete. Information gathered through the Hemisphere programme – outside statutory and constitutional procedures governing the access to phone records – effectively allows law enforcement authorities to circumvent the traditional due process clause. Given the impossibility of obtaining exculpatory information that could be related to the production of 'inaccurate, incomplete, biased or flawed evidence', the accused does not have the opportunity to counter the investigative source or method employed by the government to produce that evidence.[127] Correspondingly, defendants are deprived of their right to a 'fair proceeding'. Furthermore, intelligence laundering removes the incentive to respect statutory protections by law enforcement agents, as their actions are rendered invisible and inscrutable to the courts. According to Human Rights Watch, the resulting lack of accountability risks turning constitutional rights into little more than 'words on paper'.[128] Indeed, neither the courts nor judges can fulfil their integral function when a criminal prosecution is erected via parallel construction of the facts. The former cannot scrutinize the facts in the determination of the appropriate legal standards, whereas the latter is prevented from evaluating thoroughly the extent of the impact of intelligence practices on constitutionally protected civil liberties. Consequently, the practice of parallel construction empowers law enforcement agencies to capitalize on unprecedented streams of classified information, while obscuring the origin of that information from prosecutors, defence teams and juries.

The routine recourse to parallel construction engenders circumstances in which individuals are rendered vulnerable to investigations launched through large-scale intelligence operations, while having no means of learning about their enactment. Accordingly, the fairness of trial processes is jeopardized since the outcome of a case depends on the ability of defence attorneys to press for revelations of undisclosed methods as well as upon the willingness of prosecutors to reveal them. Overall, the use of parallel construction generates an imbalance between the extraordinary knowledge of individuals' whereabouts retained by

government agencies and the rights of individuals to know about and question such knowledge.

Concluding remarks, weaving the threads

By unearthing the procedural character behind evidence laundering, this study has sought to uncover the incongruence between the confidentiality of intelligence-gathered material vis-à-vis the open, criminal justice system. On the basis of the analysis above, it is suggested that the fundamental process underlying parallel construction is antithetical to the core of the linear justice system. From a civil liberties perspective the practice is troubling given the lack of an effective legal framework and court oversight regulating its operation. This view is reinforced by the fact that investigators possess 'manufactured jurisdiction' with regard to deciding what evidence should be introduced in a legal case vis-à-vis what should be withheld.

The circumstances are further aggravated given the absence of legal standards regulating the employment of high-tech data mining methods for security purposes. The predictive potential of Big Data has fostered a 'future-orientated approach' to the prosecution of crimes.[129] Facilitated by an environment enabling a smooth information exchange, domestic law enforcement authorities can proactively investigate ordinary criminal activities by relying on classified sources of information gathered through clandestine surveillance. Such future orientation is reinforced by the promise of algorithms to detect suspicious patterns on the feature space through a 'pattern-discovery exercise' used to justify unprecedented access to data.[130]

While there is no formal policy prescribing the proper timing for prosecutorial intervention, the most desirable point is generally at the earliest possible stage – that is, before any physical threat materializes. The legal and moral imperatives concerning whether it is best to delay a prosecution, thus maximizing the chance to collect evidence, or to intervene at the earliest possible stage with forward-leaning preventative interventions have very different consequences. The former offers the opportunity to monitor communications and learn facts critical to building the evidence-base of a criminal investigation. Indeed, the maximization of covert intelligence-gathering enhances the prospect of success at trial by yielding additional material. The latter course favours the intervention at an aspirational, rather than at the operational, stage based on the assumption of avoiding potential future harm. Nevertheless, from the 'aspirational' to the 'operational' stage the degree of suspicion is not uniform. Moving backwards from the completed criminal act through to its planning and conspiracy stages, weakens the evidentiary link between actual and anticipated harm. Hence, preventive-oriented interventions raise questions with regard to the accuracy of predictions.

In summary, law enforcement agencies have increasingly adopted a pre-crime approach to their investigations, where 'laundered' evidence derived from the large-scale collection of data is being deployed not only for national security purposes, but also to build the legal basis for domestic prosecutions. In particular, according to the scrutiny of DEA records on 'parallel construction', the areas in which classified intelligence is used for law enforcement purposes have been extended far beyond the investigation of violent political threats to national security, to encompass the dismantling of narco-trafficking organizations as well as the prosecution of minor criminal activities, such as drug violations and traffic infractions. As a result, the 'exceptionality' behind the widespread surveillance network, which looks for the proverbial needle in the haystack has been scaled-down and directed to the targeting of

regular criminal behaviours. The re-purposing of 'out of the ordinary' measures, for 'ordinary' law enforcement, in effect, produces an environment in which everyone is rendered a potential suspect. The word 'suspect' itself risks losing its substance if not confined to the criminal, juridical sense anymore.[131]

A national security framework founded on 'pre-crime' preventative measures embraces not only a 'temporal shift',[132] from the prosecution of a committed criminal act to its anticipation,[133] it also embodies a trend towards the integration of two incompatible worlds, namely, 'out of the ordinary' intelligence activities and 'ordinary, routine' law enforcement operations. Despite the attempt to reconcile the mismatch by constructing a parallel, alternative story for how investigations are launched, a fundamental incompatibility persists: whereas the former aims to be proactive in the collection of intelligence material, the latter is inherently reactive, as it responds to a committed criminal act. Framing parallel construction as an effective solution to such a discrepancy does not retroactively render them compatible. In other words, a legal framework that tries to peer into the future blurs the dividing line between evidence and intelligence.

Acknowledgements

The authors extend their grateful thanks to the reviewers and editors of the journal for their helpful comments and observations on the draft manuscript.

Disclosure statement

No potential conflict of interest was reported by the authors.

Notes on contributors

Vanessa Ugolini is a PhD student at the School of International Studies, University of Trento, Italy. Her research focuses on investigating the fracture between transnational data collection and national oversight mechanisms in the prosecution of ordinary criminal activities. She received the Barrie Paskins Award for Best MA Dissertation from the War Studies Department, King's College London, where she completed with Distinction an MA in Intelligence and International Security. She also holds a BA in Politics and East European Studies with Honours from University College London. Her research expertise cuts across critical security studies and digital surveillance techniques.

M. L. R. Smith is Research Associate in the Office of the Dean of Humanities, University of Pretoria, South Africa and Professor of Strategic Theory, King's College London. He founded the MA in Intelligence and International Security in the Department of War Studies and was its first Programme Director between 2003 and 2006. He has written extensively on issues in intelligence and international security. His work has appeared in journals such as *Intelligence and National Security, International Security, International Affairs, Review of International Studies, Orbis, Studies in Conflict and Terrorism* and *Contemporary Security Policy*.

Notes

1. US Department of Justice (Freedom of Information Operations Unit) (SARF) (2013) DEA *Intelligence Program Top-Down Review: A Partnership to Build a Premier Intelligence Program*, Performed by SAIC and ICF Incorporated, Case Number 13–00569-F, Released on November 13, 2013, 27.

2. John Shiffman and David Ingram, "Exclusive: IRS Manual Detailed DEA's Use of Hidden Intel Evidence." *Reuters*, August 7, 2013, https://www.reuters.com/article/us-dea-irs/exclusive-irs-manual-detailed-deas-use-of-hidden-intel-evidence-idUSBRE9761AZ20130807.

3. See note 2 above.

4. See Bigo, 'The Transnational Field of Computerized Exchange of Information in Police Matters and its European Guilds," 155–81.

5. Bauman et al., "After Snowden," 127.

6. Lyon, "Surveillance, Snowden, and Big Data," 3.

7. See Omand, *Securing the State*, 261–88.

8. Glenn Greenwald and James Ball, "The Top-Secret Rules That Allow NSA to Use US Data Without a Warrant." *Guardian*, June 20, 2013, https://www.theguardian.com/world/2013/jun/20/fisa-court-nsa-without-warrant.

9. John Shiffman and Kristina Cooke, "US Directs Agents to Cover Up Programme Used to Investigate Americans." *Reuters*, August 5, 2013, http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805.

10. See note 9 above.

11. Scott Shane and Colin Moynihan, "Drug Agents Use Vast Phone Trove Eclipsing NSA's." *New York Times*, September 2, 2013, https://www.nytimes.com/2013/09/02/us/drug-agents-use-vast-phone-trove-eclipsing-nsas.html.

12. Power Point: Los Angeles Hemisphere, "Synopsis of the Hemisphere Project: High Intensity Drug Trafficking Area." Released by *New York Times*, September 2, 2013, http://www.nytimes.com/interactive/2013/09/02/us/hemisphere-project.html.

13. Such requests have been submitted to the offices within the DEA Headquarters divisions located in Springfield, Virginia, Los Angeles, San Diego and San Francisco.

14. The 'Transparency Project' of the Electronic Frontier Foundation (EFF) and the Electronic Privacy Information Center (EPIC) works to obtain government records and make those records widely available to the public.

15. Adam Schwartz, “AT&T Requires Police to Hide Hemisphere Phone Spying.” Electronic Frontier Foundation, October 27, 2016, https://www.eff.org/it/deeplinks/2016/10/att-requires-police-hide-hemisphere-phone-spying.

16. Electronic Frontier Foundation (EFF), “Freedom of Information Act Request (FOIA) and Request for Expedited Processing.” Submitted to the DEA on February 5, 2014.

17. EFF, “California Public Records Act Request” (CPRA). Submitted via email to the Los Angeles Regional Criminal Information Clearinghouse (LACLEAR), May 5, 2014.

18. The letters constitute an expedited request under the Freedom of Information Act (FOIA), 5 U.S.C. § 552.

19. EFF, “Freedom of Information Act Request (FOIA) and Request for Expedited Processing.” submitted to the Drug Enforcement Administration (DEA), February 5, 2014, 3.

20. EFF, “EFF Lawsuits Seek Records About ‘Hemisphere’ Phone Call Collection and Drug Enforcement Program.” Press Release July 8, 2015.

21. The E-Government Act of 2002 requires agencies to perform Privacy Impact Assessments (PIAs) when ‘developing or procuring information technology that collects, maintains, or disseminates information that is in identifiable form’. E-Government Act of 2002, PL 107–347, December 17, 2002, 116 Stat. 2899, 208(b)(1)(A)(i)-(ii); See also M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, http://www.whitehouse.gov/omb/memoranda_m03-22.

22. A complete list of the pages that have been withheld can be found at: United States District Court, “Exemption Comparison Chart.” EFF, *Plaintiff v. Department of Justice, Defendant*, Case 3:15-cv-03186-MEJ, Document 43–2: 1–6, Filed October 3, 2016).

23. Muckrock, “DEA Policies on Parallel Construction.” Records Obtained by C.J. Ciaramella From the Drug Enforcement Administration on August 5, 2013, 1–276. Tracking Number: 13–00541-F, https://www.muckrock.com/foi/united-states-of-america-10/dea-policies-on-parallel-construction-6434/#file-15532.

24. As explained in the material gathered on the “Investigative Resources” of the Northern California Regional Intelligence Center (NCRIC) “Hemisphere – Complete NCRIC Responsive Documents” (released to EFF on 18 December 2013), slide 58 of the complete PDF document.

25. As established through the Homeland Security Presidential Directive/HSPD-8. ‘This directive establishes policies to strengthen the preparedness of the United States to prevent and respond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies by requiring a national domestic all-hazards preparedness goal, establishing mechanisms for improved delivery of Federal preparedness assistance to State and local governments, and outlining actions to strengthen preparedness capabilities of Federal, State, and local entities’. See The White House, December 17, 2003, https://fas.org/irp/offdocs/nspd/hspd-8.html.

26. See Section 1.2 of the DEA Intelligence Program Top-Down Review: "Intelligence-driven Enforcement in a Post-September 11, 2001 Environment." Freedom of Information Operations Unit (SARF), November 13, 2013, 10.

27. See note 24 above, slide 58.

28. McCulloch and Pickering, 'Pre-Crime and Counter-Terrorism,' 628–629; Aradau and Tobias, 'The (Big) Data-Security Assemblage,' 2.

29. See note 24 above, slide 95.

30. See note 24 above, slide 98.

31. See note 24 above, slide 59.

32. Speech by President George W. Bush, reporting on the recommendations of the 9/11 Commission Act of 2007. See note 24 above, slide 91.

33. Hanni Fakhoury, "DEA and NSA Team Up to Share Intelligence, Leading to Secret Use of Surveillance in Ordinary Investigations." EFF, August 6, 2013, https://www.eff.org/deeplinks/2013/08/dea-and-nsa-team-intelligence-laundering.

34. Johnny Dwyer, "The DEA's Terrorist Hunters: Overreaching Their Authority?" *Time*, August 8, 2011, http://content.time.com/time/world/article/0,8599,2087220,00.html.

35. See note 23 above.

36. See note 34 above.

37. Trevor Aaronson, "Welcome to Law Enforcement's 'Dark Side': Secret Evidence, illegal Searches and Dubious Traffic Stops." *The Intercept*, January 9, 2018, https://theintercept.com/2018/01/09/dark-side-fbi-dea-illegal-searches-secret-evidence/.

38. Peter Van Buren, "Parallel Construction: Unconstitutional NSA Searches Deny Due Process Headshot." *Huffington Post*, September 20, 2014, https://www.huffingtonpost.com/peter-van-buren/parallel-construction-unc_b_5606381.html.

39. See note 2 above.

40. See note 2 above.

41. Mike Masnick, "Parallel Construction Revealed: How The DEA Is Trained To Launder Classified Surveillance Info." *TechDirt*, February 3, 2014, https://www.techdirt.com/articles/20140203/11143926078/parallel-construction-revealed-how-dea-is-trained-to-launder-classified-surveillance-info.shtml; Louise Matsakis, "How the Government Hides Secret Surveillance Programs." *Wired*, September 9, 2018, https://www.wired.com/story/stingray-secret-surveillance-programs/.

42. Alex Wilhelm, "DEA Reportedly Hiding NSA Data Used to Prosecute U.S. Citizens." *TechCrunch*, August 5, 2013, https://techcrunch.com/2013/08/05/dea-repotedly-hiding-nsa-data-used-to-prosecute-us-citizens/.

43. See note 23 above.

44. See note 23 above, 96.

45. See note 23 above, 2.

46. Shawn Musgrave, "DEA Teaches Agents To Recreate Evidence Chains To Hide Methods." *MuckRock*, February 3, 2013, https://www.muckrock.com/news/archives/2014/feb/03/dea-parallel-construction-guides.

47. Human Rights Watch, "Dark Side: Secret Origins of Evidence in US Criminal Cases." *Human Rights Watch Report*, January 2018, 7, https://www.hrw.org/sites/default/files/report_pdf/us0118.pdf.

48. See note 23 above, 179.

49. According to interviews conducted by Human Right Watch with former federal prosecutors. For the detailed explanation. See note 47 above, 34.

50. See note 45 above, 32.

51. See note 12 above, slide 12 of 27.

52. See note 9 above.

53. See note 11 above.

54. See note 12 above, slide 5 of 27.

55. See note 9 above.

56. Aaron Mackey, and Dave Maass, "Law Enforcement's Secret 'Super Search Engine' Amasses Trillions of Phone Records for Decades." EFF, November 29, 2016, https://www.eff.org/it/deeplinks/2016/11/law-enforcements-secret-super-search-engine-amasses-trillions-phone-records.

57. See note 41 above.

58. LACLEAR Hemisphere Complete Responsive Records, Obtained by EFF through a CPRA Request, https://www.eff.org/document/hemisphere-la-clear-complete-responsive-documents.

59. See note 12 above, slide 3 of 27.

60. Paul Szoldra, "AT&T Reportedly Has a Secret Program That Helps Law Enforcement Spy Without a Warrant." *Business Insider*, October 25, 2016, https://www.businessinsider.com/att-project-hemisphere-016-10?IR=T.

61. Kris, "On the Bulk Collection of Tangible Things," 240.

62. U.S. Department of Justice (Drug Enforcement Administration) "Department of Justice's Complete Record of the Hemisphere Program," Case Number 14–00009-F. Released to Electronic Privacy Information Center (EPIC) on July 21, 2014), 1–323; U.S. Department of Justice (Drug Enforcement Administration) "Department of Justice's Complete Record of the Hemisphere Program," Case Number 14–00257-F. Released to EFF on April 7, 2015, 1–308.

63. Power Point: "Hemisphere Synopsis: Hemisphere Project Summary," Office of National Drug Control Policy, slide 12, https://www.eff.org/files/2014/09/12/7-3-14_mr6608_res.pdf.

64. See note 63 above, 13.

65. EPIC, *EPIC's FOIA Request to the DEA* (Freedom of Information Act Request, September 25, 2013); EPIC, *EPIC's Reformulated FOIA Request to DEA*, Freedom of Information Act Request, Case Number 14–00009-F, November 15, 2013.

66. U.S. Department of Justice (Drug Enforcement Administration) DEA Response Letter to EPIC, November 13, 2013.

67. US Department of Justice (Drug Enforcement Administration), "Department of Justice's Complete Record of the Hemisphere Program," Case Number 14–00009-F. Released to EPIC on July 21, 2014, 1–326.

68. LACLEAR Hemisphere Complete Responsive Records, obtained by EFF from LACLEAR (California Department of Justice) through a CPRA Request (100 pages), https://www.eff.org/document/hemisphere-la-clear-complete-responsive-documents.

69. See note 67 above, 16.

70. See note 63 above, slide 5.

71. Kenneth Lipp, "AT&T Is Spying on Americans For Profit," *Daily Beast*, October 25, 2016 https://www.thedailybeast.com/atandt-is-spying-on-americans-for-profit.

72. As released in the form of Power Point presentations: see note 12 above, slides 1–27; see also note 63 above, slides 1–24.

73. See note 63 above, slide 5.

74. See note 63 above, slide 9.

75. See note 12 above, slide 13.

76. Eric Lichtblau, "FBI Data Mining Reached Beyond Initial Targets." *New York Times*, September 9, 2007, https://www.nytimes.com/2007/09/09/washington/09fbi.html.

77. Ryan Singel, “AT&T Invents Programming Language for Mass Surveillance.” *Wired*, October 29, 2007, https://www.wired.com/2007/10/att-invents-pro/.

78. See note 76 above.

79. See note 76 above.

80. Cortes, Pregibon and Volinsky, “Communities of Interest,” 105–14.

81. See note 80 above, 10.

82. Cortes et al., “Hancock: A Language for Extracting Signatures from Data Streams,” 1–9.

83. See note 82 above, 1.

84. See note 77 above.

85. See note 82 above, 1.

86. Cortes et al., “Hancock: A Language for Analyzing Transactional Data Streams,” 1.

87. See note 86 above, 1–31.

88. See note 80 above, 105.

89. See note 80 above, 105.

90. See Aradau and Blanke, “Governing Others,” 1–21.

91. See note 80 above, 112.

92. See note 80 above, 112.

93. Predictive analytics is defined by Abbott as ‘the process of discovering interesting and meaningful patterns in data’. Abbott, *Applied Predictive Analytics: Principles and Techniques for the Professional Data Analyst*. 3.

94. Aradau and Blanke, “Politics of Prediction,” 278–379.

95. Lahneman, “IC Data Mining in the Post-Snowden Era,” 710; and Jasanoff, “Virtual, Visible, and Actionable,” 6.

96. See note 5 above, 123.

97. See note 90 above, 19.

98. Eileen Sullivan and Gene Johnson, “Drug Agents Plumb Vast Database of Call Records,” *Seattle Times*, September 2, 2013, https://www.seattletimes.com/seattle-news/drug-agents-plumb-vast-database-of-call-records/.

99. See *Katz v. United States (1967), 389 U.S. 347, 361 (Harlan, J., concurring)*. See Rapisarda, "Privacy, Technology, and Surveillance," 150.

100. See note 47 above, 4.

101. See note 47 above 11; See also Murray v. United States (1988), 487 U.S. 533, 542 (emphasis added).

102. See *Clapper v. Amnesty International USA (2013), 568 U.S. 398.*

103. See note 47 above, 53.

104. See *United States v. Pappas, 94 F.3d. 795 (2nd Cir. 1996)*; See note 23 above, 13.

105. See note 104 above, 99.

106. See note 105 above, 100.

107. See note 23 above, 17.

108. *United States v. Mejia*, 448 F. 3d 436, 457 (D.C. Cir. 2006).

109. See note 23 above, 19.

110. See note 23 above, 27.

111. See note 23 above, 25; See also *Scher v. United States'*, 305 U.S. 251 (1938).

112. See note 23 above, 276; *Scott v. United States'* (1978) 436 U.S. 128, 138.

113. See note 47 above, 41.

114. See note 47 above, 13.

115. Donohue, "Bulk Metadata Collection," 846.

116. Bartholomew, "Seize First, Search Later," 1032.

117. U.S. Constitution, Fourth Amendment (Amendment IV), Legal Information Institute, https://www.law.cornell.edu/wex/fourth_amendment.

118. Human Rights Watch telephone interview with attorney Simon Azar-Farr, San Antonio, Texas, June 1, 2017. Full Interview see note 23 above, 63.

119. See note 61 above, 228.

120. See note 76 above; see also note 115 above, 761.

121. Forsyth, "Banning Bulk: Passage of the USA Freedom Act and Ending Bulk Collection," 1313.

122. Quoted in note 76 above.

123. McCulloch and Pickering, “Pre-Crime and Counter-Terrorism,” 632.

124. Milaj-Weishaar and Bonnici, “Unwitting Subjects of Surveillance and the Presumption of Innocence,” 422.

125. US Constitution, Fifth Amendment (Amendment V), Legal Information Institute, https://www.law.cornell.edu/wex/fifth_amendment.

126. US Constitution, Sixth Amendment (Amendment VI), Legal Information Institute, https://www.law.cornell.edu/wex/sixth_amendment.

127. See note 47 above, 59.

128. See note 47 above, 2.

129. Lyon, “Big Data Surveillance: Snowden, Everyday Practices and Digital Futures,” 265.

130. See note 129 above, 6.

131. See note 5 above, 138.

132. Lennon, “Precautionary Tales: Suspicionless Counter-Terrorism Stop and Search,” 45.

133. See note 28 above, 629, 631, and 640; See also Palmer, “Dealing with the Exceptional,” 520.

134. NCRIC ‘Hemisphere – Complete NCRIC Responsive Documents’ (Released to EFF on December 18, 2013), 17.

135. Department of Justice’s Complete Record of the Hemisphere Program, Case 1:14-cv-00317-EGS, Document 15–3, Filed 09/29/14, 216.

136. Ibid., 181.

Bibliography

Abbott, D. *Applied Predictive Analytics: Principles and Techniques for the Professional Data Analyst*. Chichester: Wiley, 2014.

Aradau, C., and T. Blanke. “The (Big) Data-Security Assemblage: Knowledge and Critique.” *Big Data and Society* 2, no. 2 (2015): 1–12. doi:10.1177/2053951715609066.

Aradau, C., and T. Blanke. “Governing Others: Anomaly and the Algorithmic Subject of Security.” *European Journal of International Security* 3, no. 1 (2017): 1–21. doi:10.1017/eis.2017.14.

Aradau, C., and T. Blanke. “Politics of Prediction: Security and the Time/Space of Governmentability in the Age of Big Data.” *European Journal of Social Theory* 20, no. 3 (2017): 278–379. doi:10.1177/1368431016667623.

Bartholomew, P. “Seize First, Search Later: The Hunt for Digital Evidence.” *Touro Law Review* 30, no. 4 (2014): 1027–1052. https://digitalcommons.tourolaw.edu/lawreview/vol30/iss4/10.

Bauman, Z., D. Bigo, P. Esteves, E. Guild, V. Jabri, D. Lyon, and R. B. J. Walker. “After Snowden: Rethinking the Impact of Surveillance.” *International Political Sociology* 8, no. 2 (2014): 121–144. doi:10.1111/ips.12048.

Bigo, D. “The Transnational Field of Computerized Exchange of Information in Police Matters and Its European Guilds.” In *Transnational Power Elites: The Professionals of Governance, Law and Security*, edited by N. Kauppi and M. R. Madsen, pp. 155–181. London: Routledge, 2013.

Cortes, C., K. Fisher, D. Pregibon, R. Rogers, and F. Smith. “Hancock: A Language for Extracting Signatures from Data Streams.” *Proceedings of the Sixth International Conference on Knowledge Discovery and Data Mining* KDD20003 (2000): 1–9. doi:10.1.1.129.4786.

Cortes, C., K. Fisher, D. Pregibon, R. Rogers, and F. Smith. “‘Hancock: A Language for Analyzing Transactional Data Streams.” *ACM Transactions on Programming Languages and Systems (TOPLAS)* 26, no. 2 (2004): 1–38. doi:10.1145/973097.973100.

Cortes, C., D. Pregibon, and C. Volinsky. “Communities of Interest.” *IDA 01 Proceedings of the 4th International Conference on Advances in Intelligent Data Analysis*, no. 105–114 (September 2001). doi:10.5555/647967.741620.

Donohue, L. K. “Bulk Metadata Collection: Statutory and Constitutional Considerations.” *Harvard Journal of Law & Public Policy* 37, no. 3 (2014): 759–900. https://www.harvard-jlpp.com/vols-35-39/.

Forsyth, B. “Banning Bulk: Passage of the USA Freedom Act and Ending Bulk Collection.” *Washington and Lee Law Review* 72, no. 3 (2015): 1308–1341. https://scholarlycommons.law.wlu.edu/wlulr/vol72/iss3/9.

Jasanoff, S. “Virtual, Visible, and Actionable: Data Assemblages and the Sightlines of Justice.” *Big Data & Society* 4, no. 2 (2017): 1–15. doi:10.1177/2053951717724477.

Kris, D. S. “On the Bulk Collection of Tangible Things.” *Journal of National Security Law and Policy* 7, no. 2 (2014): 209–295. https://jnslp.com/wp-content/uploads/2014/05/On-the-Bulk-Collection-of-Tangible-Things.pdf.

Lahneman, W. J. “IC Data Mining in the Post-Snowden Era.” *International Journal of Intelligence and Counter-Intelligence* 29, no. 4 (2016): 700–723. doi:10.1080/08850607.2016.1148488.

Lennon, G. “Precautionary Tales: Suspicionless Counter-Terrorism Stop and Search.” *Criminology and Criminal Justice* 15, no. 1 (2015): 44–62. doi:10.1177/1748895813509637.

Lyon, D. “Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique.” *Big Data and Society* 1, no. 2 (2014): 1–13. doi:10.1177/2053951714541861.

Lyon, D. “Big Data Surveillance: Snowden, Everyday Practices and Digital Futures.” In *International Political Sociology: Transversal Lines*, edited by T. Basaran, D. Bigo, E.-P. Guittet, and R. B. J. Walker, pp. 254–271. London: Routledge, 2016.

McCulloch, J., and S. Pickering. “Pre-Crime and Counter-Terrorism: Imagining Future Crime in the ‘War on Terror’.” *British Journal of Criminology* 49, no. 5 (2009): 628–645. doi:10.1093/bjc/azp023.

Milaj-Weishaar, J., and J. M. Bonnici. “Unwitting Subjects of Surveillance and the Presumption of Innocence.” *Computer Law & Security Review* 30, no. 4 (2014): 419–428. doi:10.1016/j.clsr.2014.05.009.

Omand, D. *Securing the State*. London: Hurst, 2010.

Palmer, P. “Dealing with the Exceptional: Pre-Crime Anti-Terrorism Policy and Practice.” *Policing and Society* 22, no. 4 (2012): 519–537. doi:10.1080/10439463.2011.641549.

Rapisarda, M. “Privacy, Technology, and Surveillance: NSA Bulk Collection and the End of the Smith Vs. Maryland Era.” *Gonzaga Law Review* 51, no. 1 (2016): 122–158. https://gonzaga-university-law-review.scholasticahq.com/article/10064-privacy-technology-and-surveillance-nsa-bulk-collection-and-the-end-of-the-i-smith-v-maryland-i-era.