THE HAZARDS OF TECHNOLOGY-NEUTRAL POLICY: QUESTIONING LAWFUL ACCESS TO TRAFFIC DATA

.

Policies are being updated to deal with new communications infrastructures;
the path to policy renewal is fraught with danger

.

By Alberto Escudero-Pascual and Ian Hosein

To appear in Communications of ACM (Accepted 5-9-2002, Reviewed 19-10-2002)

Abstract - After some successes and many mis-steps, the regulatory environment surrounding technology policy is transforming. Lessons taken from content, copyright, and cryptography policy processes, amongst many others, resulted in the emergence of a number of technology policy innovations. Two particular innovations are the internationalization of policy-setting, and the trend towards technology-neutral policies. These innovations come with risks, however. The risks are particularly apparent when we look at policies on law enforcement access to traffic data.

Access to traffic data for law enforcement purposes is a traditional tool for investigation and intelligence gathering. *Traffic data* is an elusive term, due in part to technology variances. The policies regarding lawful access to traffic data, however, are increasingly set in technology-neutral language, while the language is often negotiated at international fora.

Each policy innovation needs to be questioned. The momentum behind the policy changes comes from both the technology and international incentive schemes. Yet the policies tend to ignore the technological details; while policy changes are argued as necessary due to international obligations. In the hope of updating our policies, we may be numbing our technological awareness and political openness.

LAW ENFORCEMENT REQUIREMENTS: THE POLITICAL

In the days of plain old telephone systems (POTS), after much legal debate, the content of communications were considered sensitive and therefore any breach of confidentiality, i.e. wiretapping required constraint, e.g. judicial warrants in the U.S., politician-authorized warrants in the United Kingdom. The same rule did not apply to *traffic data*: numbers called, calling numbers, and time. This data was considered less invasive, and therefore only required minimal constraint. That traffic data was stored by telephone companies and thus available to law enforcement authorities while communications were not, also reduced the obstacles: traffic data was available, legally less sensitive, and so accessible. This is the policy habitat [7] of traditional surveillance of communications.

The traffic data records collected by telephone companies generally look like:

[See Appendix I.A]

While the format of the logs may differ from one operator to another, the above log can identify the time and duration of a call, the phone-ID numbers involved in the call, the countries involved, and the types of service used.

The traditional investigative powers of access to traffic data were established with traditional technological environments in mind. Governments are updating their policies on interception of communications to apply to modern communications infrastructures. As cryptography policies of key escrow were mis-understood as updates 'to maintain the status quo' of government powers [9], updating legal definitions of traffic data while not acknowledging the increased 'sensitivity' of the data by claiming technological neutrality is equally problematic.

The claim of technological neutrality

Similar to the cryptography policy debates, the technological environment is now vastly different than it was when policies were first devised. Leaving aside the advances in telephone switches, we may now also communicate using a number of infrastructures including mobile telephony, Internet, and wireless LAN infrastructures. If governments insist on applying

traditional powers to these new infrastructures, the new policies must acknowledge that the data being collected now is separate from tradition.

Many policy initiatives have involved articulations regarding the importance of being technology-neutral. When the Clinton Administration first announced its intention to update lawful access powers to include cable-based internet connections, they proposed ”ammendments [that] will update the statutes in outmoded language that are hardware specific so that they are technologically neutral” [8]. Meanwhile in the United Kingdom, it was noted in the tempestuous debates in the House of Lords, regarding the Regulation of Investigatory Powers Act (RIP) 2000 that:

> The Earl of Northesk: ”One of the many difficulties I have with the Bill is that, in its strident efforts to be technology neutral, it often conveys the impression that either it is ignorant of the way in which current technology operates, or pretends that there is no technology at all.” [10]

Technology-neutral policy is seen as a way to deal with concerns of governments mandating a specific type of technology. While this is favorable in the case of some policies that affect market developments, technology-neutral lawful access policies may contain hazardous side-effects.

Another reason for technology-neutrality is to ensure that new laws do not need to be passed every time a new technology is invented. However, technology-neutral language may be used to ignore, willful or not, the challenges, risks, and costs to applying powers to different infrastructures.

DEFINING ’TRAFFIC DATA’

International governmental organizations have been working for a number of years to ensure lawful access to traffic data, including the Group of 8, Council of Europe. They have been led, through policy-modeling of or pressure from selected countries, including the United Kingdom and the United States.

The Group of 8, the ‘informal’ economic and foreign policy committee of western governments, formed a senior ‘experts’ group in 1995[1] to develop an international co-operation regime to address transnational organized crime. The Lyon Group has since been active on high-technology surveillance-related policies, including three meetings with industry representatives throughout 2000 and 2001. Arising from that work, the G8 working-definition of traffic data is ”non-content information recorded by network equipment concerning a specific communication or set of communications.” [11]

Meanwhile, the Council of Europe (CoE), the 43-member inter-governmental organization, convened closed meetings since 1997 to develop a multilateral treaty establishing lawful access powers across borders. The CoE Convention on Cybercrime defines traffic data as ”any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service” [2]. In the convention’s Explanatory Report [3], the CoE states that traffic data should be defined so as ’to not refer’ to the content of a communication; but this is a non-binding interpretation. The CoE and G8 definitions have been criticized as ambiguous and problematic, but no change has been achieved due to the closed processes of these fora.

One is left to wonder what is included and what is excluded by these vague definitions. While subject lines in emails may be content (as they ’refer to’ content [3]), uncertainty arises as to whether the name of files requested (e.g. HTTP requests), URLs (e.g. `http://www.computer.tld`), search parameters, TCP headers, and other such data are considered content or traffic data. A report of a transaction by an individual with server 158.143.95.65 may be considered traffic data; but the name of the web site(s) run on that server may disclose more information (e.g. `aidshelpline.com`). Search parameters in the URLs and the name of files accessed may refer to the content of the communications. If we consider the next generation internet, mobility bindings or routing information included in the IPv6 extended header will include location information. The location information is part of the mobility ’signaling’ protocol and hence fits into the above definitions of traffic data.

Some states have tried to deal with this challenge in their legislative language. The UK’s Regulation of Investigatory Powers Act 2001 went through many iterations, particularl y in the so-called ’Big Browser’ debate, before settling on its final terminology. Traffi c data is defined as data about the source and destination

[1] The ‘G7’ started the Lyon Group as Russia had not yet joined the group, later making it the ‘G8’.

of a transaction, and data abo ut the routing and the tying of separate packets together. This definition is complement ed by the definition of 'communications data': data attached to a transaction provided th at it is used by the network; or exists within logs; or other data that is collected by s ervice providers. However the definitions are also quite clear about the extent of inform ation that qualifies: traffic data does not include URLs per se, and may only include the name of the computers running a service, while the specific resource used qualifies as c ontent, and accorded greater protection. Therefore, the IP address is traffic data, while `http://www.url.tld/file.html` is tantamount to content.

Other states have failed to respect this level of technological awareness. Previous U.S. policy differentiated between traffic data from cable and telephone communications. The Cable Act once protected traffic data to a greater degree than telephone traffic data, as viewing habits were considered sensitive. Now that cable infrastructure is also used for internet communications (which were previously used over telephone lines, and thus traditional laws applied), successive White House administrations worked to erase this cable traffic distinction, finally succeeding with the post-September 11 USA-PATRIOT Act. Rather than deal with the specifics of digital communications media and services, the changes in U.S. law reduces the protections of traffic data for cable internet communications to what had previously existed for telephone communications data. The terminology within the U.S. Code is now ambiguous, lacking supporting documentation with elaborate definitions, and is therefore quite similar to the terms within CoE and the G8 documentation.

This can be interpreted as a boon to law enforcement. According to Attorney General Ashcroft:

> Agents will be directed to take advantage of new, technologically neutral standards for intelligence gathering. (...) Investigators will be directed to pursue aggressively terrorists on the internet. New authority in the legislation permits the use of devices that capture senders and receivers addresses associated with communications on the internet [1].

Traffic data blurs with the content of communications as new communications infrastructures are encompassed under existing practices. The legal protection of this data is reduced as distinctions applied are based on categorical decisions established under older technologies. The separation of content and traffic remains elusive, even in policy language.

Categorical Determinants: The technological

Traffic data under the plain old telephone system was considered derivative, and while informative, it did not necessarily disclose the sensitive details of an individual's life. While the Cable Act protections accepted that the data discloses the viewing preferences of individuals and therefore deserved greater protections, such protections were later deemed irrelevant for the internet.

Traffic data's constitution differs by communications medium. Below we present dial-in records, wireless LANs, and search engines to preview what can accessed by technology-neutral law enforcement powers.[2]

Dial-In records

The Remote Authentication Dial-In User Service (RADIUS) is a client/server security protocol, designed to manage dispersed modem pools for large numbers of users. This tends to involve managing a single "database" of users, which allows for authentication (verifying user name and password) as well as configuration information detailing the type of service to deliver.

Many Internet Service Providers are outsourcing the access network to big operators that provide dial-up connectivity world-wide. Internet users dial into a modem pool attached to a Network Access Server (NAS) that operates as a client of RADIUS. The client is responsible for passing user information to designated RADIUS servers (managed by the ISP) and then acting on the response that is returned.

The RADIUS server stores usage information for dial-in users, often for billing purposes. When the user is authenticated and the session has been configured according to the authorization information, an accounting start record is created. When the user's

[2]The data presented has been obtained with permission from a telephone carrier, an internet service provider, and a large conference where wireless LAN access was provided. All transactions presented in this paper have been de-identifi ed, and the time-logs were altered to reduce the risk of re-identifi cation.

session is terminated, an accounting stop record is created.

The most significant fields of the ”start/stop” records are:

- *Timestamp:* Timestamp records the time of arrival on the RADIUS accounting host measured in seconds since the epoch (00:00 January 1, 1970 GMT). To find the actual time of the event, subtract Acct-Delay-Time from Timestamp.

- *Call(ed,ing)-Station-Id:* Where the Called-Station-Id records the telephone number called by the user and the Calling-Station-Id records the number the user is calling from. This information is recorded when the NAS-Port-Type is ISDN, ISDN-V120, or ISDN-V110.

Start and stop RADIUS records may look like:

[See Appendix I.B]

From this log we can extract a limited amount of information regarding the content of the communications transactions that took place. The user has been identified (aep@somedomain.org), the number of the caller (01223555111, which is a Cambridge number) and the place being called (02075551000, London), IP address assigned (62.188.17.227), the duration (21s), type of connection, date and time. The traffic data over time identifies the change in location of a user despite the common dialed number. As users roam globally with different access telephone numbers, the user identification remains static. In this sense, the collected traffic data is mildly more sensitive than traditional telephone data: where POTS traffic data pivots around a given telephone/ID number, RADIUS data pivots around a user ID regardless of location; therefore disclosing location shifts.

Wireless LAN association records

Such mobility becomes more problematic within wireless environments. In a standard wireless LAN environment using IEEE 802.11b, a radio cell size can vary from hundreds of meters in open air, to a small airport lounge. Before the mobile station (STA) is allowed to send a data message via an access point (AP), it must first become associated with the AP. The STA learns what APs are present and then sends a request to establish an association.

The significant records of a centralized association system log are:
- *time_GMT:* Time when a mobile node associates with a base station
- *Cell_ID:* Base station unique identifier in the LAN
- *MAC_ID:* Media Access Control address identifier; a unique Identifier of a mobile device

[See Appendix I.C]

It is tempting to analyze these logs by drawing an analogy with the POTS, i.e. a registration of a mobile with an access point could be seen as the establishment of a phone call between both parties. This analogy is simplistic as it doesn’t consider that the Cell_IDs represent places (airport, conference room, restaurants) and the registration timestamps can reveal if two nodes are (moving) together. Data mining of association records (registration and deregistration) can provide sufficient information to draw a map of human relationships. [4]

HTTP requests to a search engine

The above media may involve further traffic data in the form of internet protocols. The GET and POST methods in the Hypertext Transfer Protocol (HTTP) allow a web client to interact with a remote server. In the most common search engines, the keywords are included in the HTTP header as part of a GET method. All the web logs can be transformed to a W3C common log file format that contains the IP address of the client, the connection time, the object requested and its size.

[See Appendix I.D]

If ’traffic data’ residing in logs are accessed by authorities, a great deal of intelligence can be derived. Observing the logs we can see for example, that 212.164.33.3 has requested (in a short period of time) information about ”railway+info+London” and ”union+strike” in two different requests. This is the ability to find out not only the patterns of an individual’s movements on-line, but also to identify an individual’s intentions and plans. Or more dangerously one could derive false intentions (child+pornography may be a search for studies on the effects of pornography on children). Much more can be ascertained with some datamining, even if IP addresses are assigned dynamically, allowing for traceability based on habits

and interests; and compounded with location data, previous NAS data, etc., a comprehensive profile can be developed.

THE SHAPE OF THINGS…

Even the Council of Europe acknowledges, within the convention's Explanatory Report [3], that the breadth of possible traffic data may be problematic.

> "The collection of this data may, in some situations, permit the compilation of a profile of a person's interests, associates and social context. Accordingly Parties should bear such considerations in mind when establishing the appropriate safeguards and legal prerequisites for undertaking such measures."

No such safeguards or prerequisites are discussed in detail, or mandated as, again, the Explanatory Report is non-binding and often ignored.

Shifting between infrastructures gives different data; but converging infrastructures is even more worrisome. Mobile communications systems magnify the sensitivity of traffic data; wireless LANs were presented as an indication of the shape of things to come as we encounter new protocols and infrastructures, e.g. third generation wireless running IPv6.

This exposition of traffic data could be extended to mobile telephony; and to understanding the output of devices such as Carnivore (DCS1000); the point can be made that the data collected depends on both the infrastructure and the means of collection. The collection and access methods currently under consideration are preservation (access to specified data of a specific user that are collected by service providers for business purposes), retention (requiring all logs for all users be stored beyond their business purpose for government access), and real-time (governmental access to real-time data flows).

The national laws that enshrine these access powers differ remarkably, despite being established under the umbrella/guidance of international organizations such as the G8 and the CoE. The UK appears to separate URLs from traffic data; but in the same piece of legislation assured that ministers sign interception warrants, and in later policies and legislation proposed retention regimes for periods of time ranging from 4 days (web cache), 6 months (RADIUS, SMTP, and IP logs), and 7 years [5]. The U.S. recently introduced technological-neutrality to its laws thus reducing protections; but the U.S. does require judicial warrants for interception, and has no retention requirements. The CoE convention places no requirements on countries to require judicial authorizations, and with 33 signatory states including the U.S., Canada, South Africa, Romania, France, and Croatia, we can rest assured that there will be selective interpretation in implementation. Even among the G8 countries, the protections afforded to citizens' communications in Italy, Germany, the U.S. and Russia vary greatly. Already the Canadian government has proposed, in its efforts to ratify the CoE convention, to consider all telecommunications services as equivalent, and argues that "the standard for Internet traffic data should be more in line with that required for telephone records and dial number recorders in light of the lower expectation of privacy in a telephone number or Internet address, as opposed to the content of a communication." [6]

While policies may vary within and across borders, the nature of the data produced and its sensitivity does not. 'Traffic data' analysis generates more and more sensitive profiles of an individual's actions and intentions, arguably more so than communications content. In a communication with another individual, we say what we choose to share; in a transaction with another device, e.g. search engines and cell stations, we are disclosing our intents, actions, and movements. Policies continue to regard this transactional data as plain old telephone system 'traffic data', and accordingly apply old protections.

This is not faithful to the spirit of updating laws for new technology. We need to acknowledge that changing technological environments alter the habitat of a policy. New policies need to reflect the totality of the new environment.

The technology policy innovations fail to do so. Governments seek technology-neutral policy, and are also doing so at the international level. This appears to be to the advantage of policy-setters. New powers are granted through technological ambiguity rather than clear debate and due process. International instruments, such as those from the Group of 8 and the Council of Europe, harmonize language in a closed way with little input and debate. This problem will grow as more countries feel compelled to ratify and adopt these instruments; or feel that it is in their interests to do so.

Attempts to innovate policy must be interrogated, lest we reduce democratic protections and oversight blindly.

About the Authors

Ian (Gus) Hosein is a Visiting Fellow in the Department of Information Systems at the London School of Economics; and a Senior Fellow at Privacy International. For more information please see http://is.lse.ac.uk/staff/hosein/

Alberto Escudero Pascual is a Research Assistant in the Telesystems Laboratory at the Royal Institute of Technology (KTH) in the area of privacy in the next generation Internet. For more information please see http://www.it.kth.se/~aep/

References

[1] Ashcroft, J. Testimony of the Attorney General to the Senate Committee on the Judiciary. Washington D.C. September 25, 2001.

[2] Council of Europe. Convention on Cybercrime, ETS no.185, opened for signature on November 8, 2001. http://conventions.coe.int/

[3] Council of Europe. Convention on Cybercrime Explanatory Report, adopted on November 8, 2001. http://conventions.coe.int/

[4] Escudero A. Contribution to the EU Forum on cybercrime. Location data and traffic data. Brussels. November 2001.

[5] Gaspar, R. Looking to the Future: Clarity on Communications Data Retention Law: A National Criminal Intelligence Service submission to the Home Office for Legislation on Data Retention. Submitted on behalf of ACPO and ACPO(S); HM Customs & Excise; Security Service; Secret Intelligence Service; and GCHQ, August 2000.

[6] Government of Canada. Lawful Access - Consultation Document. Department of Justice, Industry Canada, Solicitor General Canada. August 25, 2002.

[7] Hosein, I., and Whitley, E. ”Developing national strategies for electronic commerce: Learning from the UK’s RIP Act.” Journal of Strategic Information Systems, Volume 11, Number 1, 2002.

[8] Podesta, J. National Press Club Speech with (former) White House Chief of Staff John Podesta on ”Cyber Security”. Washington D.C. July 17, 2000.

[9] Reno, J. Law Enforcement in Cyberspace Address by The Honorable Janet Reno, (former) United States Attorney General. San Francisco: Presented to the Commonwealth Club of California, 1996

[10] UK Hansard. ”House of Lords 28th June, 2000 (Committee Stage)”, Column 1012 (published by The Stationery Office Limited).

[11] U.S. Delegation to G8. Discussion Paper for Data Preservation Workshop. Tokyo, G8 Conference on High-Tech Crime. May 22-24 2001.

I. Appendix

A. CDR

The call data records look like:

```
19991003070824178 165 0187611205 46732112106 ----------001------003sth 46 4673000-----0013 14 10260
1999100307083041 33 01541011341 46708314801 ----------001------003sth 46 4670000--8 0013 11 10260
1999100307162963 51 0187614815 46739112106 ----------001------003sth 46 4673000-----0013 13 10260
1999100307182788 74 015410124301 46708314801 ----------001------003sth 46 4670000--8 0014 11 10260
1999100307204736 18 0187614805 46739112106 ----------001------003sth 46 4673000-----0013 14 10260
1999100307222326 20 01317023888 46706263087 ----------001------003sth 46 4670000--6 0013 1 10260
1999100300131791 90 0131654200 46854543084 ----------001------002sth 46 46 001-----0014 14 10260
```

Fig. 1. Call Data Records

B. Radius Records

A start and stop radius records looks like:

▹ ***Fri Oct 19 11:30:40 2001***
User-Name = ”aep@somedomain.org”
NAS-IP-Address = 62.188.74.4
NAS-Port = 3239
NAS-Port-Type = Async
Acct-Status-Type = Start
Acct-Delay-Time = 0
Acct-Session-Id = ”324546354”
Acct-Authentic = RADIUS
Calling-Station-Id = ”01223555111”
Called-Station-Id = ”02075551000”
Framed-Protocol = PPP
Framed-IP-Address = 62.188.17.227
Proxy-State =
”PX01\0\0‘\0xcdntg\0x13\0xfe\0xfe\0xdd+ew\0xdfV\0xa4\0xc7Y\[...]\0xfc\0x8c”

▹ ***Fri Oct 19 11:31:00 2001***
User-Name = ”aep@somedomain.org”
NAS-IP-Address = 62.188.74.4
NAS-Port = 3239
NAS-Port-Type = Async
Acct-Status-Type = Stop
Acct-Delay-Time = 0
Acct-Session-Id = ”324546354”
Acct-Authentic = RADIUS
Acct-Session-Time = 21
Acct-Input-Octets = 11567
Acct-Output-Octets = 3115
Acct-Input-Packets = 96
Acct-Output-Packets = 74
Calling-Station-Id = ”01223461172”
Called-Station-Id = ”9061000”
Framed-Protocol = PPP
Framed-IP-Address = 62.188.17.227
Proxy-State = ”PX01\0\0\0x1b\0x93;\0xaa\0x98\0xea\0xad\[...]\0xc7\0xffi”

Fig. 2. Radius Data Records

From the previous log we can extract the following information:
User: aep@somedomain.org
Place of call: Cambridge (UK) 01223555111
Calling to: London (UK) 02075551000
IP address: 62.188.17.227
Durantion of call: 21 Seconds
Type of connection: ASYNC MODEM
Date and time: from Fri Oct 19 11:30:40 2001 to Fri Oct 19 11:31:00 2001

C. WLAN Authentication Records

WLAN authentication records looks like:

```
time_GMT=20010810010852 Cell_ID=115 MAC_ID=00:02:2D:20:47:24
time_GMT=20010810010852 Cell_ID=115 MAC_ID=00:02:2D:04:29:30
time_GMT=20010810010852 Cell_ID=115 MAC_ID=00:60:1D:21:C3:9C
time_GMT=20010810010853 Cell_ID=129 MAC_ID=00:02:2D:02:40:EF
time_GMT=20010810010854 Cell_ID=129 MAC_ID=00:02:2D:1F:53:C0
time_GMT=20010810010854 Cell_ID=129 MAC_ID=00:02:2D:09:17:E8
time_GMT=20010810010854 Cell_ID=129 MAC_ID=00:02:2D:1D:67:FE
time_GMT=20010810010856 Cell_ID=41 MAC_ID=00:02:2D:0A:5C:D0
time_GMT=20010810010856 Cell_ID=41 MAC_ID=00:02:2D:1F:78:00
time_GMT=20010810010856 Cell_ID=41 MAC_ID=00:60:1D:1E:D4:53
time_GMT=20010810010858 Cell_ID=211 MAC_ID=00:60:1D:F0:E4:D8
time_GMT=20010810010900 Cell_ID=154 MAC_ID=00:30:65:00:62:27
time_GMT=20010810010900 Cell_ID=154 MAC_ID=00:02:2D:05:0B:25
time_GMT=20010810010900 Cell_ID=154 MAC_ID=00:60:1D:22:26:A7
time_GMT=20010810010900 Cell_ID=154 MAC_ID=00:02:DD:30:06:90
time_GMT=20010810010900 Cell_ID=154 MAC_ID=00:02:2D:0D:27:D3
```

Fig. 3. WLAN Authentication Records

D. HTTP Search Engine Queries

Extracting search queries from a web log we can obtain records that look like:

```
295.47.63.8 - - [05/Mar/2002:15:19:34 +0000] "GET /cgi-bin/htsearch?confi g=htdigx&words=startrek HTTP/1.0" 200 2225
295.47.63.8 - - [05/Mar/2002:15:19:44 +0000] "GET /cgi-bin/htsearch?confi g=htdig&words=startrek+avi HTTP/1.0" 200 2225
215.59.193.32 - - [05/Mar/2002:15:20:17 +0000] "GET /cgi-bin/htsearch?confi g=htdig&words=Modem+HOWTO HTTP/1.1" 200 2045
192.77.63.8 - - [05/Mar/2002:15:20:35 +0000] "GET /cgi-bin/htsearch?confi g=htdig&words=conflict+war HTTP/1.0" 200 2225
211.164.33.3 - - [05/Mar/2002:15:21:32 +0000] "GET /cgi-bin/htsearch?confi g=htdigx&words=railway+info HTTP/1.0" 200 2453
211.164.33.3 - - [05/Mar/2002:15:21:38 +0000] "GET /cgi-bin/htsearch?confi g=htdigx&words=tickets HTTP/1.0" 200 2453
211.164.33.3 - - [05/Mar/2002:15:22:05 +0000] "GET /cgi-bin/htsearch?confi g=htdigx&words=railway+info+London HTTP/1.0" 200 8341
212.164.33.3 - - [05/Mar/2002:15:22:35 +0000] "GET /cgi-bin/htsearch?confi g=htdigx&words=union+strike HTTP/1.0" 200 2009
82.24.237.98 - - [05/Mar/2002:15:25:29 +0000] "GET /cgi-bin/htsearch?confi g=htdigx&words=blind+date HTTP/1.0" 200 2024
```

Fig. 4. HTTP Search Engine Records

Observing the logs we can see for example, that *212.164.33.3* has requested (in a short period of time) information about “railway+info+London” and “union+strike” in two different requests.