

Understanding Traffic Data and Deconstructing Technology-neutral Regulations

Ian Hosein
<i.hosein@lse.ac.uk>

Department of Information Systems
The London School of Economics
and Political Science
London, UK

Alberto Escudero Pascual
<aep@kth.se>

TSLAB - IMIT
Royal Institute of Technology (KTH)
IT University
Stockholm, Sweden

7th March 2002

Abstract

Initiatives to update traditional powers of investigation involving technology do not always reflect the sensitivities raised by the current technological environment. In this paper we review the common policy initiative to extend traditional powers of access to communications traffic data, designed for the plain old telephone system, for mobile telephony, internet communications, and wireless local area networks. We will then present some of the data that may qualify as traffic data from these communications infrastructures, to show the varying level of details that can be derived from that data.

As new technology-neutral policies are implemented, we argue that this is increasingly dangerous as traffic data granularity affects the sensitivity of the data collected. To conclude, we propose that lawful access policies must be technology-specific, and as a result governments must consider protecting the right of privacy of an individual's traffic data equally to that of communications.

1 Introduction

Traditional investigative powers were established with traditional technological environments in mind. When telephone traffic data was decided to be less invasive than the content of the conversation, this reflected the plain-old-telephone system (POTS): traffic data was merely the person who was calling or the person called, and the duration. Accordingly, one level of privacy protection was typically assigned to traffic data (if at all), and another was applied to lawful access to communications content, that is, the conversation itself.

National policies regarding lawful access to traffic data and communications content are now being updated as the technological environment is now vastly different than it was when policies were first devised. If governments insist on applying traditional powers to these new infrastructures, we argue that the new lawful policies must acknowledge that the data being collected now is separate from tradition.

Many policy initiatives have involved articulations regarding how the policy must be technology-neutral. When the Clinton Administration first announced its intention to update lawful access powers to include cable-based internet connections, they proposed "amendments [that] will update the statutes in outmoded language that are hardware specific so that they are technologically neutral" [1]. Meanwhile in the United Kingdom, it was noted in the tempestuous debates in the House of Lords, regarding the Regulation of Investigatory Powers Act (RIPA) 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." (28 Jun 2000 : Column 1012)[2]

One reason for technology-neutral policy was a way to deal with the concerns of governments mandating a specific type or form of technology [3]. While this is favourable in the development of some policies that affect market developments, e.g. to ensure choice and variability in the marketplace, technology-neutral lawful access policy is more problematic.

Another reason for technology-neutrality is to ensure that new laws do not need to be passed every time a new technology is invented [4]. Although it seems logical, this reasoning presented by policy-makers may be specious; one can not have the mandate of updating laws for new technologies then in the same breath argue against updating for the next new technology and thus require technology-neutral policy. It is our contention that technology-neutral language may be used to ignore, wilfull or not, the challenges, risks, and costs to applying powers to different technical infrastructures.

This paper is divided as follows: Section 2 contains an overview of the status of different policies on traffic data and the organisations working on them. Section 3 lists some of the privacy concerns when defining traffic data in a technology-neutral way. Section 4 includes a set data records that may qualify as traffic data from different communications infrastructures, to show the varying level of details that can be derived from that data and Section 5 presents some conclusions and regulatory recommendations.

2 Lawful access to traffic data policies

National governments and international organisations have been working for a number of years to update or enhance policies on traffic data, and often implemented in a technology-neutral way. Without giving a complete review of the various policy instruments (and they are frequently changing, particularly after September 11, 2001), we will present a few examples of how traffic data is being defined, particularly in international fora, and discuss some of the arising challenges.

The Group of 8 Industrialised Countries (G8) established a subcommittee, the Lyon Group, to work on international co-operation regimes in order to address transnational organised crime. The Lyon Group has been active in recent years on surveillance related policies, including a number of meetings with private sector representatives throughout 2000 and 2001. In that work, the G8 defines traffic data as the *"non-content information recorded by network equipment concerning a specific communication or set of communications. Traffic data includes the origin of a communication, the duration, the nature of the communication activity (not including content) and its destination. In the case of Internet communications, traffic data will almost always include an IP address and port number."* [5]

While the Lyon Group was meeting with industry representatives, the Council of Europe (CoE), the 43-member state organization, was convening closed meetings to develop a multilateral treaty establishing procedural 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."* [7] In the convention's Explanatory Report [8], 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.

Both of these above definitions appear to apply to **all forms of communications media**; and encompasses all data apart from (or 'not including' (G8), or 'does not refer to' (CoE)) the communications content. However 'communication' remains undefined in both fora; and would therefore apply to all forms of transactions and their underlying service. In the traditional definition of communication, involving postal mail or telephone conversations, traffic data was a log of communications sent or received, sometimes including information that would identify recipients and senders. This new definition-regime involving auxiliary information and consideration to the underlying service recognizes the richer data which the expanded use of technology has now made available.

One is left to wonder what is included and what is excluded by these vague definitions. "That is, while subject lines in emails appear to be content (as they 'refer to' content [7]), uncertainty arises as to whether the name of files requested (e.g. HTTP requests), URLs (e.g. <http://www.computer.tld>), search key words, IP addresses, 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 give over more information (e.g. aids helpline.com), nearer to the amount of information disclosed by monitoring the URLs. Search parameters in the URLs, such as <http://www.google.com/search?q=aids+homosexuality>, however, and the name of files accessed (*GET aids/gifs/lesion.gif*) may refer to the content of the communications. If we consider the next generation internet, mobility bindings or routing information included in the IP_{v6} extended header will include location information as the home and roaming networks. The location information is part of the mobility "signaling" protocol and hence fits into the current definition of traffic data [6].

The CoE does acknowledge, within the convention's Explanatory Report [8], 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.

Some states have tried to deal with this challenge in their legislative language. The United Kingdom’s Regulation of Investigatory Powers Act (RIPA) went through many iterations before settling on its final terminology (which is still open for debate within Codes of Practices). Traffic data is defined as data about the source and destination of a transaction, and data about the routing and the tying of separate packets together. This definition is complemented by the definition of ‘communications data’, which is traffic data attached to a transaction provided that it is used by the network; or exists within logs; or other data that is collected by service providers. However the definitions are also quite clear about the extent of information that can be qualified as ‘traffic’: traffic data does not include URLs per se, and may only include the name of the computers running a service (*www.google.com*), while the specific resource used qualifies as content (*search?q=aids+homosexuality*). This interpretation is consistent with the ideal interpretation of the CoE definition, as the ‘traffic data’ (google request) does not refer to the content (file names, search parameters).

Other states have failed to respect this level of technological awareness. Previous U.S. policy, for example, differentiated between traffic data on cable and telephone communications. The Cable Act traditionally protected traffic data to a higher degree than telephone traffic data. Now that cable infrastructure is used for internet communications (which were previously used over telephone lines, and thus traditional laws applied), successive White House administrations have tried to erase this distinction, and reduce the protections in the Cable Act – and this occurred in the post-September 11 USA-PATRIOT Act. Rather than deal with the specifics of digital communications media and services, the changes to the U.S. law introduced by the Patriot Act reduced the protections of traffic data for all communications to what had previously existed for telephone communications data, thereby ignoring technological differences. 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. The separation of content and traffic remains elusive, even in policy language.

3 Privacy concerns of technical neutrality when applied to “traffic data”

The technology-neutral approach may serve not only to expand the types of data that are accessed under a weak regime of protection, but also create a shift in the perception of the process of collection.

There are concerns, however, that in certain contexts a "technology-neutral" approach may lead to situations in which the surveillance laws become "content-neutral." In other words, in the quest for "technology-neutrality," the focus may become not on whether the information being gathered is content or not content, but rather on whether the information gathered can be obtained by a certain technology, such as that capable of capturing "routing" or "addressing" information that may contain elements of content but which might be gathered from the Internet with a pen register or trap and trace device [9].

The separation of content and traffic becomes increasingly blurred by this approach, while the due process requirements are further reduced by more recent legislation, particularly the USA-PATRIOT Act 2001. 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 [10].

That is, traffic data blurs with the content of communications as new communications infrastructures are encompassed under existing practices, and the protection of this data is reduced as different procedures apply based on categorical decisions established under the plain old telephone system.

| N | Type of record | pos | format |
|----|------------------------------------|-----|-----------------------------------|
| 1 | Date of the call | 8 | <yymmdd> |
| 2 | Start of the call | 6 | <hhmmss> |
| 3 | A leg duration of the call | 10 | <seconds> |
| 4 | B leg duration of the call | 20 | <seconds> |
| 5 | Flag for customer identification | 2 | - |
| 6 | A number | 20 | <number> |
| 7 | Misc, defined in field | 2 | - |
| 8 | B number | 40 | <number> |
| 9 | Customer ID | 20 | - |
| 10 | Carrier | 3 | <internal def> |
| 11 | Cost | 12 | <xx.yy> |
| 12 | Service | 3 | 001=itl, 002=domestic, 003=mobile |
| 13 | Switch ID | 10 | - |
| 14 | Origin country | 4 | 46=Sweden |
| 15 | Destination country | 4 | [1st-4th digit] |
| 16 | Bearer service indicator | 3 | 000=speech 001=UDI |
| 17 | Tele Service Indicator | 3 | |
| 18 | Destination country | 6 | [5th-10th digit] |
| 19 | Flag for identification of field 7 | 2 | 00=A-number, 01=Freephone |
| 20 | In trunkgroup | 3 | |
| 21 | Out trunkgroup | 3 | |
| 22 | Pointcode | 5 | |
| 23 | CR+LF | 2 | |

Table 1: CDR records format

4 The Technology and the Data

Specifically we are going to investigate traffic data and show how traffic data changes depending on the infrastructure. Four sources of records has been studied from real data.

1. Call data records from plain-old-telephone system (POTS).
2. Internet dialup Radius accounting records.
3. Wireless lan access point association records.
4. Internet HTTP GET search engine records.

The data presented below 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-identified, and the time-logs were altered to reduce the risk of re-identification.

For each of sources we present a short description of the service monitored, the format of the records and the amount of personal information that can be extracted from them.

4.1 CDR from POTS

The main source of traffic data from the plain-old telephone system (POTS) are the Call Data Records (CDR) which contains basic information for accounting and billing. The format of the CDRs differ from one of operator to another but all of them contain the start time of the call, the duration, the calling and called number and type of call

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
1999100307252533 23 01554456033 46705942916 -----001-----003sth 46 4670000-----5 0013 1 10260
199910022155379952 9950 0114442912 46114704900 -----001-----002sth 46 46 000-----0013 13 10260
1999100223592713 11 0154852329 468313809 -----001-----002sth 46 46 000-----0013 13 10260
19991003000033156 155 0191453500 46317730252 -----001-----002sth 46 46 001-----0014 14 10260
1999100300013159 56 01317674480 468280193 -----001-----002sth 46 46 000-----0014 14 10260
19991003000445135 134 0165236800 4665118988 -----001-----002sth 46 46 001-----0014 14 10260
19991003001043123 122 0165056800 4665118988 -----001-----002sth 46 46 001-----0014 14 10260
199910030011125579 5575 01347764480 4687934300 -----001-----002sth 46 46 000-----0014 14 10260
19991003001117239 238 0131612200 46317037475 -----001-----002sth 46 46 001-----0013 14 10260
199910030012333 1 01844765475 4697874038 -----001-----002sth 46 46 001-----0014 13 10260
1999100300131791 90 0131654200 46854543084 -----001-----002sth 46 46 001-----0014 14 10260

```

4.2 Dialup RADIUS records

The Remote Authentication Dial-In User Service (RADIUS) is a client/server security protocol created by Lucent InterNetworking Systems [11]. Radius has been designed to manage dispersed modem pools for large numbers of users. Since modem pools are by definition a link to the outside world, they require careful attention to security, authorization and accounting. This can be best achieved by 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 to the user.

Many Internet Service Providers are outsourcing the access network to big operators that provide dial-up connectivity world wide.

Internet users dial into pool of modems 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 which is returned.

RADIUS servers are responsible for receiving user connection requests, authenticating the user, and then returning all configuration information necessary for the client to deliver service to the user. The radius server stores usage information for dial-in users. This information is often used 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 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). This attribute provides a machine-friendly version of the logging time at the beginning of the accounting record. To find the actual time of the event, subtract Acct-Delay-Time from Timestamp.

Call(ed,ing)-Station-Id Called-Station-Id records the telephone number called by the user. Calling-Station-Id records the number the user is called from. This information is recorded when the NAS-Port-Type is ISDN, ISDN-V120, or ISDN-V110 where supported by the local telephone company.

NAS-Port-Type NAS-Port-Type records the type of port used in the connection. The port type can be any of the following: Async, Sync, ISDN, ISDN-V120, or ISDN-V110.

PPP-Framed-IP IP address provided to user during the PPP negotiation

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 = "01223461172"
Called-Station-Id = "9061000"
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"
```

From the previous log we can extract the following information:

```
User: aep@somedomain.org
Place of call: Cambridge (UK) 01223461172
Calling to: London (UK) 9061000
IP address: 62.188.17.227
Duration 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
```

4.3 Wireless lan association records

A wireless local area network (LAN) is a flexible data communications system implemented as an extension to, or as an alternative for, a wired LAN. Using radio frequency (RF) technology, wireless LANs transmit and receive data over the air, minimizing the need for wired connections. Thus, wireless LANs combine data connectivity with user mobility.

In a standard wireless lan environment using IEEE 802.11b a radio cell size can vary for some hundreds meters in an open air to be as small as a lecture room or an 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 send a request to establish an association.

The most significant records of a centralized association system log are:

time_GMT GMT time when a mobile node associates to a base station

Cell_ID Base station unique identifier in the LAN

MAC_ID Media Access Control address identifier of the mobile node interface

And the 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
```

We could be tempted to analyze these logs by drawing an analogy between MAC_ID and Cell_ID and Calling-Station-id and Called-Station-id (i.e. the AP association is equivalent to a phone call between the mobile node and the AP). This analysis is not enough, if we consider that Cell_IDs represent places (airport, conference room, restaurant) where a set of mobile devices are in a certain time. Data mining of association records can provide with enough information to draw the map of human relationships without any other extra information [12].

4.4 HTTP requests to a search engine

The Hypertext Transfer Protocol (HTTP) is an application protocol that runs at the top of TCP/IP that provides a the set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web.

The HTTP GET method, allows a web client to interact with a remote server. If we consider the case of a search engine, the keywords are included in the HTTP header as part of the GET method.

All the web logs contain at least the IP address of the client, the connection time, the object requested and its size and the protocol version used for the request.

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

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.

5 Conclusions and recommendations

Lawful access to communications are protected because of a reasonable expectation of privacy and because of the attribution of sensitivity to such interactions. Many countries, but not all with the UK being a notable exception, therefore require judicial warrants before granting access to these communications to law enforcement agencies. Traffic data, originally conceptualised under the POTS was considered a less invasive technique because the amount of information disclosed was limited. However, the changing technological environment has altered this policy habitat significantly.

We have investigated two worrying trends. First, governments are updating their legislative frameworks to deal with new communications infrastructures; but they are tending towards ambiguous, or technology-neutral terminology, particularly in defining traffic data. Second, we have shown that ‘traffic data’ differs for each communications infrastructure and protocol, and the amount of information that can be deduced from this

information increases as we look to more sophisticated communications media than the POTS. The policy language developed under POTS and sustained through 'technology-neutral' policy intentions now gives law enforcement agencies access to highly sensitive data; but only under the protections afforded to the more benign POTS procedures. In fact, 'traffic data' appears to be more 'interaction data' in which we can learn the details of an individuals intentions, thoughts, and interests; and in a sense is more sensitive than the contents of communications.

If governments insist on applying traditional powers to these new infrastructures, we argue that the new lawful policies must acknowledge that the data being collected now is separate from tradition. It is our opinion rather that technology-neutral policy is often to the advantage of the policy-setters as new powers are granted through ambiguity rather than clear debate and due process. Attempts to be technology-neutral should be interrogated, lest in our blindness we reduce democratic protections and oversight under the deterministic veil of progress.

Acknowledgements

We will like to acknowledge Richard Clayton and Caspar Bowden for their assistance in clarifying the treatment of traffic data in RIPA 2001.

About the Authors

▷ **Ian (Gus) Hosein** is a Visiting Fellow in the Department of Information Systems at the London School of Economics; Senior Fellow of Privacy International; Technology Policy Advisor to Zero-Knowledge Systems; and a member of the Foundation for Information Policy Research advisory council. His research interests include international co-operation and mutual legal assistance in criminal matters, jurisdiction and regulation, and privacy and technology. For more information please see <http://is.lse.ac.uk/staff/hosein>

▷ **Alberto Escudero Pascual** has been doctoral student at the Royal Institute of Technology (KTH) in Sweden since January 2000. He obtained a Lic. Ph.D. Degree (2001) in the subject of location privacy in mobile internet. His special research interests have been wireless internet access, privacy and security in mobile internet, privacy-enhancing technologies and privacy threats in the next generation Internet. For more information please see <http://www.it.kth.se/~aep/>

I am certainly not an advocate for frequent and untried changes in laws and constitutions. I think moderate imperfections had better be borne with; because, when once known, we accommodate ourselves to them, and find practical means of correcting their ill effects. But I know also, that laws and institutions must go hand in hand with the progress of the human mind. As that becomes more developed, more enlightened, as new discoveries are made, new truths disclosed, and manners and opinions change with the change of circumstances, institutions must advance also, and keep pace with the times. We might as well require a man to wear still the same coat which fitted him when a boy, as civilized society to remain ever under the regimen of their barbarous ancestors."

Thomas Jefferson, to Samuel Kercheval, July 12, 1810

References

- [1] Podesta, J. National Press Club Speech with White House Chief of Staff on "Cyber Security". Washington D.C. July 17, 2000.
- [2] UK Hansard. "House of Lords 28th June, 2000 (Committe Stage)." (published by The Stationery Office Limited)
- [3] Winn, J. K. "Open Systems, Free Markets, and Regulation of Internet Commerce." Tulane Law Review 72(1177).
- [4] Ministers of the EU. Global Information Networks: Ministerial Declaration. Bonn, European Union. 6-8 July 1997.
- [5] US Delegation. Discussion Paper for Data Preservation Workshop. Tokyo, G8 Conference on High-Tech Crime. May 22-24 2001

- [6] Escudero, A. Tutorial: Location Privacy in IPv6: 'Tracking binding updates'. IDMS2001. Lancaster. UK. September 2001.
- [7] Council of Europe. Convention on Cybercrime, ETS no. 185, opened for signature on November 8, 2001. <http://conventions.coe.int/>
- [8] Council of Europe. Convention on Cybercrime Explanatory Report, adopted on November 8, 2001. <http://conventions.coe.int/>
- [9] Taylor, P. "Issues Raised by the Application of the Pen Register Statutes to Authorize Government Collection of Information on Packet-Switched Networks." Virginia Journal of Law and Technology. Spring 2001.
- [10] Ashcroft, J. (2001). Testimony of the Attorney General to the Senate Committee on the Judiciary. Washington DC. September 25, 2001.
- [11] Rigney, C. et al. Remote Authentication Dial In User Service (RADIUS). RFC 2138
- [12] Escudero A., Contribution to the EU Forum on cybercrime. Location data and traffic data. Brussels. November 2001.