



iBorrow

laptop borrowing scheme

iBorrow Technical Report (Data Collection)

Andy Powell
30.9.2009

JISC

ucisa
Award for Excellence
Winner 2009

 Canterbury
Christ Church
University

Table of contents

| | | |
|----------|--|----------|
| 1 | INTRODUCTION | 3 |
| 1.1 | Management Summary:..... | 3 |
| 2 | REQUIREMENTS..... | 3 |
| 2.1 | Data Requirements..... | 3 |
| 2.1.1 | Device Data..... | 3 |
| 2.1.2 | Location data / extraction [Mobility Services Engine]..... | 4 |
| 2.1.3 | Login data..... | 4 |
| 2.1.4 | Ethics data | 4 |
| 2.1.5 | Research data [output]..... | 5 |
| 2.1.6 | Server requirements / Data store | 5 |

1 Introduction

1.1 Management summary:

“iBorrow will allow users of a new Library and Learning Centre to borrow a notebook computer as easily as picking a book from a shelf. It will provide a large-scale demonstration of how thin-client notebooks with location-aware technology can enable the University to not only provide no-fuss access to a full range of software and learning resources but also effectively manage the configuration of the facilities within the large flexible learning spaces of its new learning centre. By overlaying location information with additional data it can also provide insights into the way students use electronic and virtual resources at an individual level or within a group context and thus answer the questions that arise when designing new learning spaces.”

<<http://www.jisc.ac.uk/whatwedo/programmes/institutionalinnovation/iborrow.aspx>>
taken 3-Sept-2009

This document outlines how the data will be collated and summarise the process that will be used to provide the raw data required.

2 Requirements

2.1 Data requirements

Various data were required to answer the research questions, namely; user information, device information and location. Data was taken from numerous sources to make up the research which was analysed by the researchers. For example, a user’s login (username) determines the ethically approved data which was retrieved but the user’s login details were not retained.

It was important to understand that preventing Data Protection Act (DPA) infringement was a fundamental part of the design of the data collection process. Whilst the ethics approved data was sufficiently generic that, in itself it did not infringe DPA principles, the process to get to that data did involve (for a period of time, no more than 24 hours,) the collection and use of personal data. This personal data, the loginID, was used to connect the location of the mobile device to the ethics-approved data. Once this connection (an extraction of data) had occurred, the personal data was irrevocably disposed of, so the only data that was retained was compliant with the Ethics Approval.

2.1.1 Device data

As we controlled the 200 iBorrow devices (Atom-based netbooks) that were tracked, we knew the Mac Address of the wireless Network Interface Adapter. This data was sourced from user technology when the devices were imaged. The information gathered was:

| Data | Example |
|---------------|-------------------|
| Computer Name | C600NNNNN |
| Mac Address | 00:00:00:00:00:00 |

It was important to make sure that we only tracked the 200 iBorrow devices rather than other mobile devices. The list of devices, a static list, was held in a table called “iBorrowdevices”; the list did not need to be maintained (may also need to exist in an XML file also).

2.1.2 Location data / extraction [Mobility Services Engine]

In order to know a device’s location , Network Services purchased a hardware device, “Cisco 3300 Series Mobility Services Engine” (MSE), which allowed an Application Programming Interface (API) to query where devices were within the Augustine House. While the MSE allowed x y coordinates, it was configured to the zones within the building which were used in the reporting (for example each floor had about six zones). The API allowed code to query where the 200 iBorrow devices were rather than extracting every device that the MSE was aware of (which would include staff / student laptops and any wireless device in the building); this made it easier to extract the required data. We queried the MSE at five minute intervals in order to find out the device locations. This generated 57,600 records a day (12 [5 minute] slots in an hour multiplied by 24 hours multiplied by 200 devices). Over the six months of the project the total data collected was in the region of 10 million rows (assuming full usage).

Data that was extracted:

| Data | Example |
|---------------|-------------------|
| Mac Address | 00:00:00:00:00:00 |
| Location Zone | W1B |

A timestamp was added to each record, enabling the data to be analysed over time.

2.1.3 Login data

In order to comply with auditors requirements, every user login and logout events on the active directory are recorded (server / database / table = cmac-nhr-01 / service_ad / logins). We used this data to calculate the user on the device at the time of querying. In the same store of logins we hold the device’s name and Internet Protocol (IP) addresses. We can take the device’s IP address and work out the Mac address from the DHCP system (server / database / table = db-nhr-01 / dhcp / ipallocations).

2.1.4 Ethics data

The research required information about the device user at the point of use outline in the “Education Faculty Research Ethics Review” document (found on Blackboard):

| Data | Example |
|------------------------------|--------------------------------------|
| Level of study | Undergraduate or postgraduate |
| Type of undergraduate degree | Single or joint honours |
| Subjects studied | Major and minor subjects |
| Year of undergraduate study | Year 1, year 2 etc. |
| Age | |
| Disability | Yes or no, not details of disability |
| Gender | |

| | |
|-------------------------------|-------------------------------------|
| Mode of attendance | Full time, part time etc |
| Postcode of student residence | Only the first half, CT1 or ME1 etc |
| Campus where student is based | Canterbury, Medway etc |

The data was provided by Corporate Information Services (CIS), who collate it on behalf of the Registry. The data was only collected for students; staff and associates data was not retrieved.

The login data was recorded contemporaneously at the poll interval (e.g. every five minutes) but the mapping to ethics data happened once per 24 hour period. This was for two reasons; (i) it was unreasonable to repeatedly and so frequently pull data from the Corporate Information Systems, (ii) the ethics data did not churn sufficiently fast that a collecting interval of less than 24 hours would have improved it. Every night the login data was mined for list of unique loginIDs which were then used to pull the ethics data which were written against all the rows of data for each unique loginID. Once completed, the loginID information was irrevocably destroyed.

2.1.5 Research data [output]

Data provided to the research committee was:

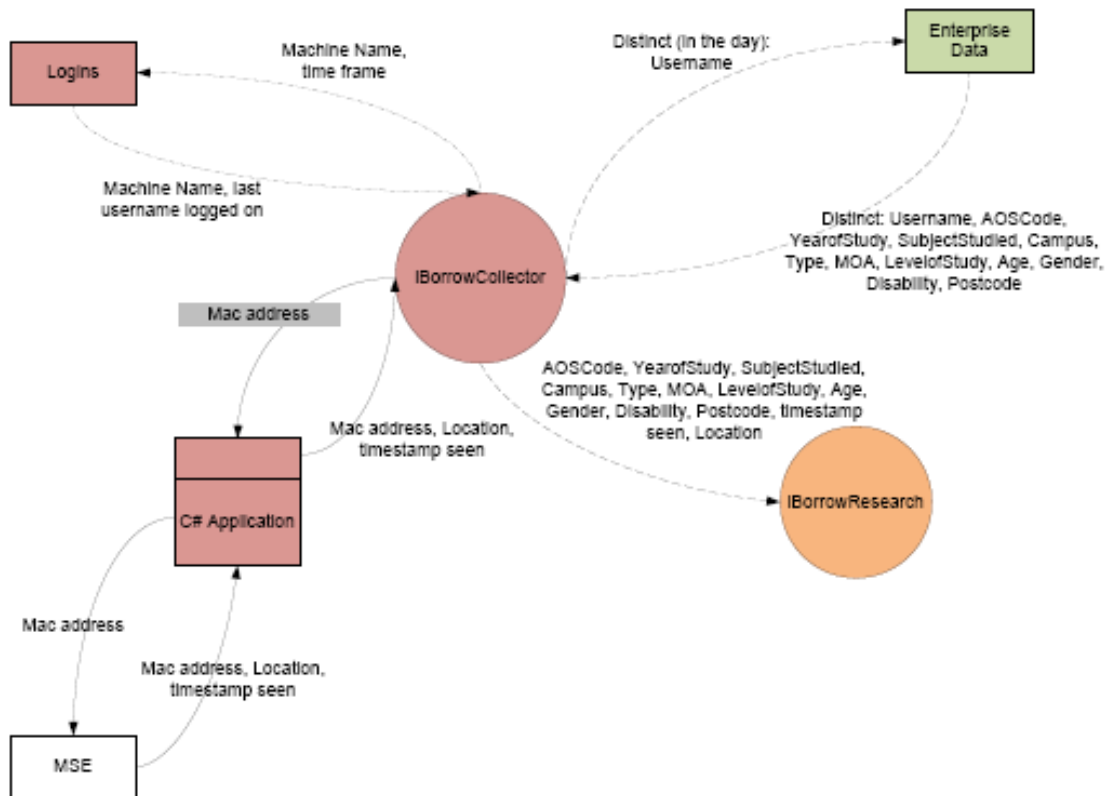
| Data | Source |
|-------------------------------|--|
| Location zone | Location data / extraction [Mobility Services Engine] |
| Time stamp | Location data / extraction [Mobility Services Engine] (point of data entry). |
| Level of study | Ethically-approved data |
| Type of undergraduate degree | Ethically-approved data |
| Subjects studied | Ethically-approved data |
| Year of undergraduate study | Ethically-approved data |
| Age | Ethically-approved data |
| Disability | Ethically-approved data |
| Gender | Ethically-approved data |
| Mode of attendance | Ethically-approved data |
| Postcode of student residence | Ethically-approved data |
| Campus where student is based | Ethically-approved data |

The data, in a single table, was built at the time of recording.

2.1.6 Server requirements / data store

The data was collated on an SQL server that already existed and a data feed to external tools will be available (Microsoft Access [adp] / Microsoft Excel).

Process Diagram



| DB Locations | |
|---|----------------------|
| | CMAC-NHR-01 |
| | DB-NHR-01/production |
| | DB-NHR-01 |

| Line Key | |
|----------|-----------------|
| ----- | Nightly |
| ————— | 5 minutes |
| ————— | 5 minutes timer |

Mac address This information has been provided by User technology.

IBorrowCollector This will only hold the collector information for 48 hours, and then purge the data.