

Introducing the Secure Data Service

A new vision for secure data access in the UK

Richard Welpton

SENIOR DATA AND USER SUPPORT OFFICER
SECURE DATA SERVICE
UK DATA ARCHIVE
UNIVERSITY OF ESSEX





Secure Data Service OUR MISSION

To promote excellence in research by enabling safe and secure remote access by bona fide researchers to data heretofore deemed too sensitive, detailed, confidential or potentially disclosive to be made available under standard licensing and dissemination arrangements

Data Access Before the SDS

For more than 40 years, the UK Data Archive has operated a number of different data access regimes

- **Open access** / anonymous download – public use
- **End User Licence** – scientific use data
- **Special Conditions** – scientific use data, sensitive
- **Special Licence** / Approved Researcher – restricted data

The Data Feeding Frenzy

Data Liberation Front

Cloud Computing

**MEAT
MEAT
MEAT**

Let's Google Map It!

Publicly funded should mean publicly available

Millions of benefits records lost

**Laptop with official secrets
left on train**

Data CDs sent in post LOST

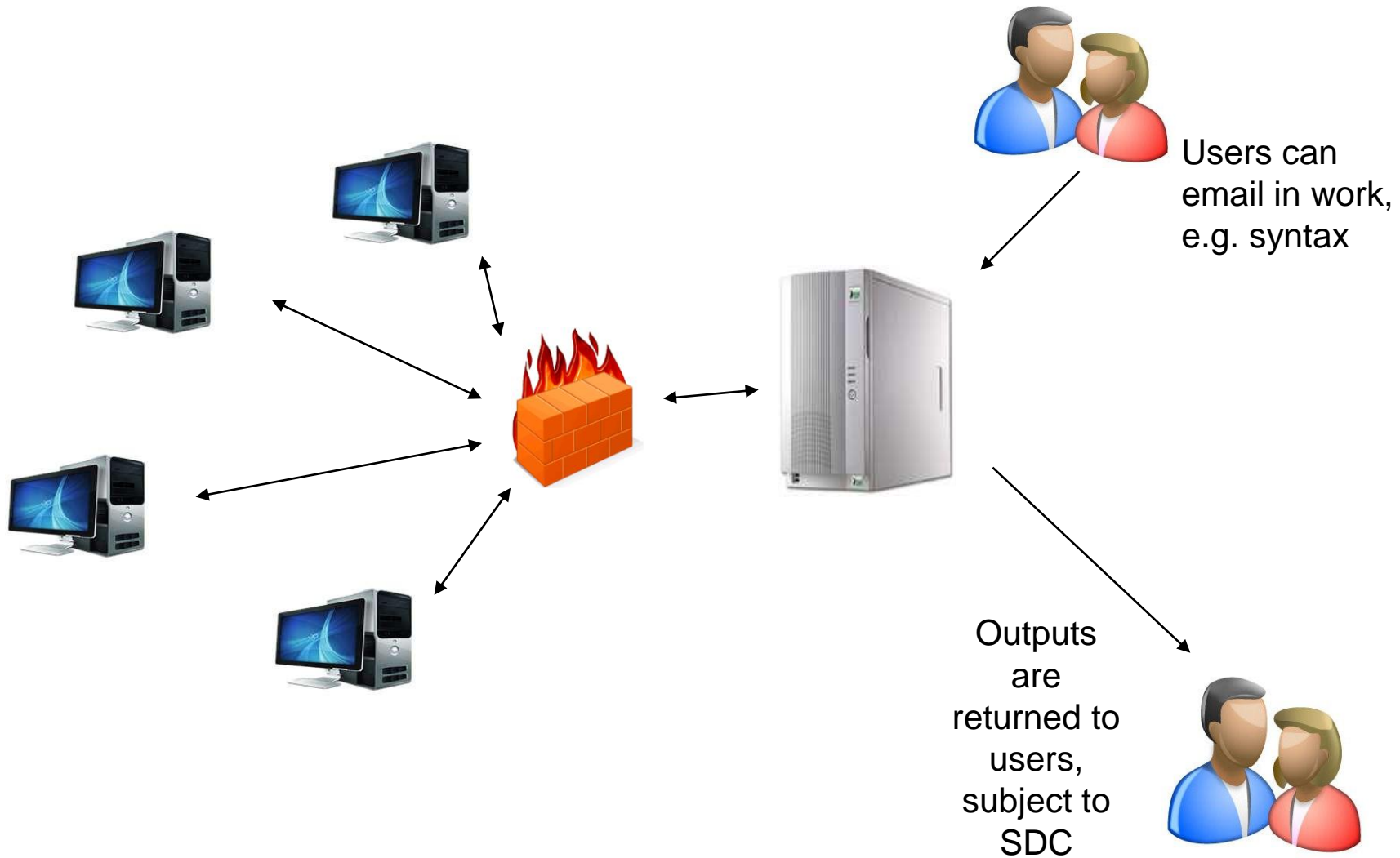
Identity Theft on the Rise

Census "resisters" organise

Opportunities

- Statistics and Registration Services Act (2007)
 - **Rights** (replaces the £1 contract!)
 - Unprecedented **access** to official data about individuals to “approved researchers”
 - **Responsibilities**
 - **Penalties** (hefty fines and custodial sentences)

What is the SDS?



SDS Security Model: Principles

- anonymisation → Safe data
 - valid statistical purpose → Safe project
 - trusted researchers → Safe people
 - technical controls around data → Safe setting
 - disclosure control of results → Safe output
- ⇒ safe use**

- *-After Ritchie, 2006*

SDS Security Philosophy - Carrots

Carrots (data providers):

- Provides remote access (securely)
- Increased data security
- Maximises data collection resources

Carrots (users)

- Desktop access to sensitive micro-data
- Providing familiar tools in a familiar environment
- Free training on disclosure control and data

SDS Security Philosophy – Big Sticks

Sticks:

- Penalties policy with real teeth:
 - **suspending access** to the system
 - **denying access** to all data from the Data Archive
 - **denying access** to any ESRC-funded research resource
 - denying future ESRC **research funding**
 - **fining and custodial sentences** (if in breach of statistics legislation)
- Penalties can be imposed both on individuals and on their **entire institution**



SDS – Back Office

- **Data held securely on firewalled SDS servers**
- Connection via Citrix™ VPN **secure remote access** technology
- User access:
 - **Desktop**
 - **Remote secure room** (standards set and agreed between SDS and data owner)
 - **Remote secure machine**
- **SmartAuditor** allows us to monitor users
- **No data allowed out**; all outputs SDC vetted before release

What Data is/will be Available?

- Detailed social data (e.g. BHPS with grid references)
- ONS VML business data
 - Subject to agreement – finalised October 2010
 - E.g. gva, innovation, R&D, Ecommerce, earnings, capital stocks
 - Linkable (panel, sources) via unique refs
- Other ESRC-funded studies
 - (social sciences, qualitative)
- Other suppliers – we're happy to negotiate for access!

User Journey: who can use it?

- Anybody with access to the JANET network
 - e.g. Academics
- Access from a UK institution

But not.....

- Civil servants, other non-academics (at least until 2012)

User Journey – Gaining Access

- User identifies SDS data – drop in '**shopping basket**'
- User applies to become:
 - **Approved Researcher** (for data covered under Statistics legislation) or
 - **ESRC Accredited Researcher** (for other secure data)
- **Data owners** (or designated authority) **grant or deny** permission
- User completes **training session** (Legal, SDC, SDS)
- User signs **agreement to terms and conditions** of use of service and gets user ID and password for remote access

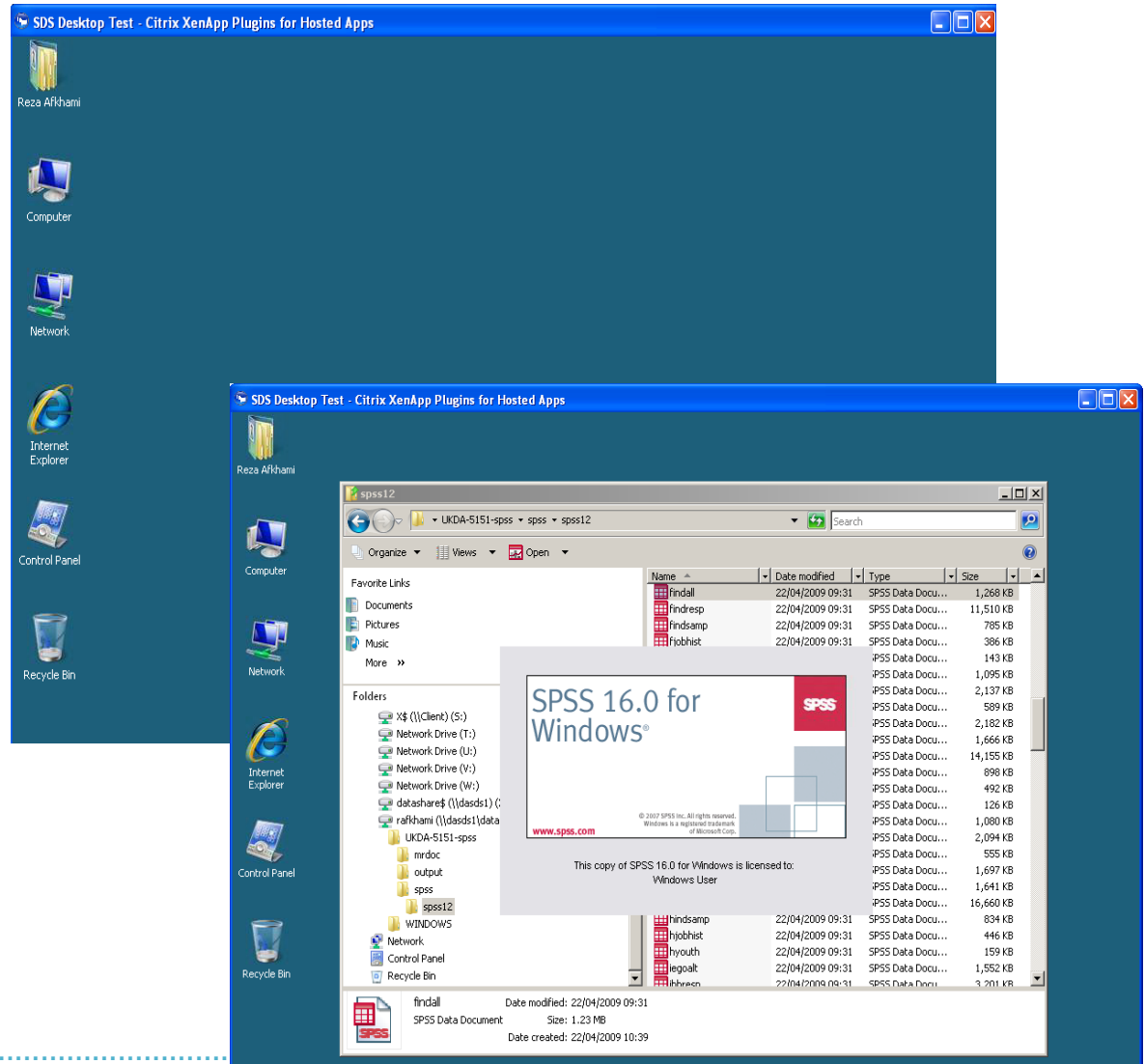
User Journey – Using the System

Users access the system remotely, either from their desktop on an approved network (ie JANET) or, for some data, from a remote secure room



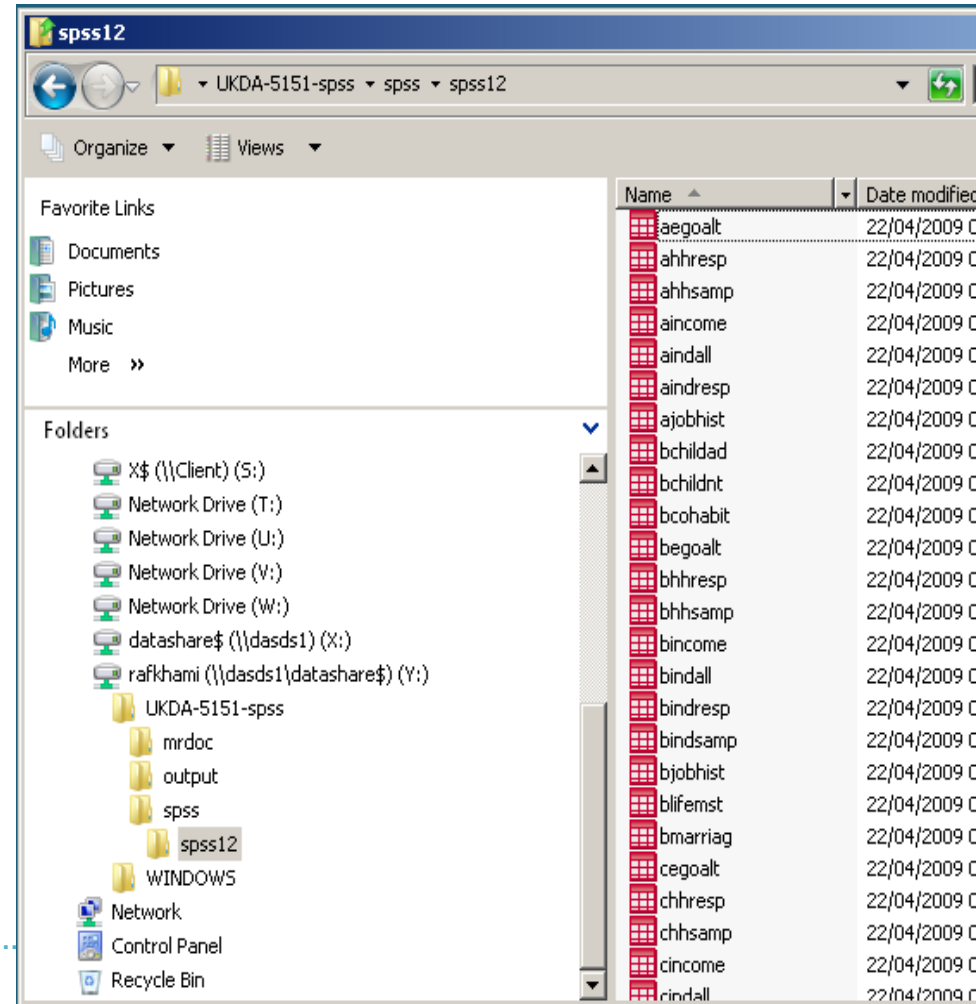
User Journey – Using the System

Citrix™ presents user with a “home away from home” familiar desktop with their data, the statistical and office tools they are familiar with (SPSS, Stata, Word, Excel, etc)



User Journey – Using the System

- Projects allotted common collaborative spaces for drafting papers, sharing interim outputs (all project members must be approved for same data sources)
- Users allowed to bring in data from standard Data Archive collection and other data sources (if approved and subject to checks)



User Journey – Using the System

- Users leave everything on the server until final outputs for publication required, which are then vetted by SDS staff (and data owners, if they wish)
- System allows remote locking for inactivity, remote shut down for suspicious keystrokes





Thank You

securedata@ukda.ac.uk

<http://securedata.ukda.ac.uk>

SECURE DATA SERVICE
UK DATA ARCHIVE
UNIVERSITY OF ESSEX
WIVENHOE PARK
COLCHESTER
ESSEX CO4 3SQ
+44 (0)1206 874968, (0)1206 873528

UK DATA ARCHIVE