WMG Service Systems Research Group
Working Paper Series

HAT Briefing Paper 6
Personal Data Exchange Ecosystem: Code of Practice Release 1

ISSN: 2049-4297
Issue Number: 03/16

About WMG Service Systems Group

The Service Systems research group at WMG works in collaboration with large organisations such as GlaxoSmithKline, Rolls-Royce, BAE Systems, IBM, Ministry of Defence as well as with SMEs researching into value constellations, new business models and value-creating service systems of people, product, service and technology.

The group conducts research that is capable of solving real problems in practice (ie. how and what do do), while also understanding theoretical abstractions from research (ie. why) so that the knowledge results in high-level publications necessary for its transfer across sector and industry. This approach ensures that the knowledge we create is relevant, impactful and grounded in research.

In particular, we pursue the knowledge of service systems for value co-creation that is replicable, scalable and transferable so that we can address some of the most difficult challenges faced by businesses, markets and society.

Research Streams

The WMG Service Systems research group conducts research that is capable of solving real problems in practice, and also to create theoretical abstractions from or research that is relevant and applicable across sector and industry, so that the impact of our research is substantial.

The group currently conducts research under six broad themes:

- Contextualisation
- Dematerialisation
- Service Design
- Value and Business Models
- Visualisation
- Viable Service Systems and Transformation

WMG Service Systems Research Group Working Paper Series
Issue number: 03/16
ISSN: 2049-4297
March 2016

HAT Briefing Paper 6
HAT Personal Data Exchange Ecosystem: Code of Practice Release 1

Service Systems Group
Warwick Manufacturing Group,
University of Warwick, Coventry CV4 7AL, UK.
E-mail: sswmg@warwick.ac.uk

Acknowledgement: The authors gratefully acknowledge the funding contribution of Research Council (UK) Digital Economy to the HAT project (http://hubofallthings.org) grant reference EP/K039911/1 which has contributed substantially to the research conducted in this paper.

If you wish to cite this paper, please use the following reference:

HAT Project Research Team (2016) HAT Personal Data Exchange Ecosystem: Code of Practice Release 1. WMG Service Systems Research Group Working Paper Series, paper number 03/16, ISSN 2049---42

HAT Personal Data Exchange Ecosystem: Code of Practice Release 1

TABLE OF CONTENTS

VERSION CONTROL

This HAT Code of Practice is effective from November 2015. It supersedes all previous versions of the Code of Practice.

HAT Personal Data Exchange Ecosystem: Code of Practice Release 1

1. Executive Summary

The HAT as a multi-sided market would enable participants such as HAT Personal Data Platform Providers (HPPs) and HAT Application Providers (HAPs) with HAT-ready services and HAT-ready devices and HAT Users to leverage on the network effects in the HAT personal data exchange ecosystem to create value for all participants. In order to develop and sustain the multi-sided market, three forms of architecture would be leveraged: the technological architecture (design, see HAT Briefing Paper 4[1]), activity architecture (activities required for operating the platform, HAT Briefing Paper 2) and value architecture (set of values; HAT Briefing Paper 1). In this process, the newly formed HAT Foundation (see HAT Briefing Paper 5), taking over from the HAT research project team would play the role of governance body for the multi-sided market market involving strategic decision-making, platform and economic model design (incentives and revenue structure) and generating governance rules. This Briefing Paper 6 concentrates on documenting the key governance rules implemented through the **Five Key HAT Operating Principles, HAT Code Of Practice, HAT Information Policies and Certification Checklist**.

2. HAT Operating Principles

The HAT Foundation holds the following fundamental beliefs. First, in the personal data economy, the way to deal with negative externality of personal data such as privacy and confidentiality concerns is to allow individuals to claim their personal data from the collectors (mainly the firms). While firms may still hold the individual's data, it is the aspiration of the HAT ecosystem that when HATs are ubiquitous, firms would only need to synchronise their data with individual HATs, and may not, in the future, actually store them. Second, user information privacy is the utmost priority. For information privacy, we take the user-centric approach and deem privacy as generated in the whole data journey (collection, transferring, storing, analysis and dissemination) in the personal data ecosystem. Therefore, the confidentiality and security issues concerning personal data would be controlled by the HAT User. Third, the HAT Foundation deems leveraging the three forms of architecture (technology, activity and value) as crucial for the development and viability of the multi-sided market. Fourth, among the three architecture forms, value co-creation for all participants is essential to drive the HAT ecosystem. This means that the individual also has the freedom to manipulate, organise and bundle their data in any way. Finally, the HAT Foundation regards the key to determining success for the HAT ecosystem to be the regulation and governance rules such as the HAT privacy principles (HAT Briefing Paper 3), technology (HAT Briefing Paper 4), processes such

[1] All HAT Briefing Papers can be downloaded at http://hubofallthings.com/hatoutputs/hat-briefing-papers/

as auditing and certification, and the regulatory roles of the HAT Foundation. These beliefs would be manifested and implemented in the following principles:

HAT PRINCIPLE 1	HAT Personal Data is owned by the HAT User
HAT PRINCIPLE 2	Access to HAT User Personal Data is controlled by the HAT User
HAT PRINCIPLE 3	Usage of HAT Personal Data is controlled by the HAT User
HAT PRINCIPLE 4	The Value of the **HAT Marketplace** is driven by the HAT Participants
HAT PRINCIPLE 5	HAT-ready Devices, HAT-ready Services and HAT Service Providers are **HAT Compliant** by supporting the other **HAT Principles** implemented by the **HAT Information Policies**

Next, we document the HAT Code of Practice and HAT Information Policies for governing the activities of participants in the HAT personal data ecosystem.

3. HAT Code Of Practice

The HAT Code of Practice ("CoP") provides information on the HAT policies and practices to which all HAT Participants should comply. This CoP is maintained by the HAT Foundation that has been created to support the HAT principles and governance trust framework of the HAT Marketplace. The HAT CoP includes the following items:

3.1 Global Privacy Standards

The HAT CoP represents Global Privacy Standards that apply to all HAT Participants in the HAT data exchange ecosystem. This includes the HAT information Policies that define the conduct and use of HAT data and its exchange between HAT Participants. These are universal policies that apply to all HAT Data exchange activity and are designed to support HAT Participants in enabling the HAT sharing principles and privacy approach. The HAT Foundation acts as a governance oversight to ensure that HAT Participants comply with the HAT Information Policies. The value of the HAT ecosystem is driven by these Global Privacy Standards to enable HAT transactions that flatten data and connect HAT Users and HAT Service Providers in a HAT Marketplace. Where there exist local privacy and security rules within national boundaries, the HAT ecosystem participants will have to adhere to the local rules.

3.2 Scope and Consent for Personal Data

The HAT CoP describes the collection, use, disclosure, retention and protection of the HAT User's personal data. This includes the conditions of use of personal data established in the HAT Information Policies. A HAT User has control over the access, use and conditions of use of HAT Data. This enables HAT Users to provide consent to Opt-in or Opt-out of sharing their personal data.

3.3 Information Policy

The HAT CoP defines the HAT personal data-sharing philosophy and principles of working that enable the HAT Marketplace. HAT Service Providers are required to comply with the HAT Information Policies and this forms part of the HAT Certification process. This then becomes the HAT Code of Conduct for those HAT Service Providers to maintain compliance with the HAT Information Policies.

3.4 Collection

The HAT CoP defines the collection of personal data and the form in which this data is held. It represents the HAT Data that is subject to the HAT Information Policies in the way it is collected, used and exchanged by HAT Users and HAT Service Providers. Privacy and confidentiality are key HAT principles and upheld in the collection of personal HAT Data with HAT-Ready Devices and HAT-Ready Services.

3.5 Use and Retention

The HAT CoP defines the policies for use of personal HAT Data by HAT Service Providers and HAT Users. It defines how HAT Data is retained by HAT Service Providers and in the way the HAT Data is used to enable the HAT User's personalisation experience. This includes offering HAT Users services that they may like, contact them about their account and services, provide them with customer service, personalised advertising and marketing and detect, prevent, mitigate and investigate fraudulent or illegal activities.

Personal data is retained by HAT Service Providers based on the information policies concerning HAT User retention. HAT Service Providers may retain HAT User Data from closed accounts to comply with national laws, prevent fraud, collect any fees owed, resolve disputes, troubleshoot problems, assist with any investigation, enforce the HAT User Agreement and take other actions permitted or required by applicable national laws.

3.6 Data Sanitation

The HAT CoP defines the policies for data removal and data destruction if a HAT User requests that their HAT Data be removed or moved to another HAT Service Provider. This also includes HAT Service Provider data cleansing to take steps to remove HAT Data after the HAT Data exchange has been completed.

3.7 Choice in Sharing

The HAT CoP defines policies of how HAT User personal information is shared by the Opt-in/Opt-out rules specified by the HAT User for their HAT Data. This is to enable control by the HAT User in the choice of how they communicate their HAT Data to other HAT Participants. It also includes the choice about how HAT Service Providers use their personal information to communicate with them, send them marketing information and provide them with personalised advertising, and whether they want to stay signed in to their account.

3.8 Access Control

The access to HAT Data will be included in the HAT CoP which defines requirements for HAT Service Providers to enable the HAT User to authorise and control how their HAT Data is accessed and by whom. It requires HAT Service Providers to take steps to ensure that the personal information collected is accurate and up to date, and that the HAT Users have the ability to access it and make any necessary corrections.

3.9 Exchange

The HAT CoP defines policies that affect how HAT Data is exchanged between the HAT User and HAT Service Providers. This includes the HAT Data exchange between HAT-to-HAT Providers, which may include HAT Data transactions or the movement of a Personal HAT's Data from one HAT Service Provider to another.

3.10 Disclosure & Consent

The HAT CoP includes policies that require disclosure of how HAT personal information is used by the HAT Service Provider and with other HAT Service Providers or with third parties outside the HAT Marketplace. This disclosure will include how the HAT Service Provider will provide a HAT User access to HAT Services, to comply with the HAT Service Provider's own legal obligations, to enforce the HAT User Agreement, to facilitate HAT Service Provider marketing and advertising activities, or to prevent, detect, mitigate and investigate fraudulent or illegal activities related to HAT Services. This also includes consent from the HAT User required for a HAT Service Provider to disclose their personal information to third parties for marketing and advertising purposes only with the HAT User's explicit consent.

3.11 Notification

The HAT CoP includes policies on how HAT Participants are notified of their events and other information that may be Opt-in/Opt-out or general events in the HAT Marketplace. This includes communications of HAT Service Provider notifications to a

specific HAT User or HAT Users (such as notification of marketing events, new HAT services or changes to existing HAT services.) This will include HAT User notifications to HAT Service Provider or Providers such as request of changes to HAT Data usage or Opt-in/Opt-out changes.

3.12 Security

The HAT CoP includes policies that are guidance on how HAT User personal data is protected, using technical and administrative security measures to reduce the risks of loss, misuse, unauthorised access, disclosure and alteration. HAT Service Providers offer safeguards in managing HAT personal data such as firewalls and data encryption, physical access controls to HAT Data centres, and information access authorisation controls.

3.13 Important Information

The HAT CoP includes important information specific to the use of the HAT Service. This includes:

- What happens when HAT Users share their personal information on HAT sites or applications
- How HAT Users should use the information they receive from the HAT
- How to respond to unwanted emails
- Third party privacy practices outside the HAT ecosystem

3.14 Third-Party Privacy Practices

This HAT CoP addresses only the use and disclosure of HAT personal information collected from the HAT Users and its usage by HAT Participants. If HAT information is disclosed to others, or if HAT Users are directed to a third---party website, their privacy notices and practices will apply.

The privacy or security of the HAT User's information is not guaranteed once the HAT User provides it to a third party, and HAT Users are encouraged to evaluate the privacy and security policies of their trading partner before entering into a transaction and choosing to share their information. This applies even when personal information is disclosed by a HAT Service Provider or HAT Application to third parties.

4. HAT Information Policies

HAT Information Policies support the **Five Key HAT Operating Principles.** These are the key features of the HAT Trust Framework and the Terms of Use of the HAT. The HAT Information Policies are necessary for all *HAT Participants* to successfully *implement the HAT vision*. The *HAT Information Policies* define the *responsible actions and outcomes required by HAT Service Providers* in order to achieve *HAT Certification*. The specific HAT Information Policies that implement the HAT Principles are the following rules. These *policies apply to HAT roles* such as HAT Platform Providers (HPP), HAT Application Providers (HAP), HAT Developers and other HAT Service Providers.

HAT INFORMATION POLICY 1 – Definition Of Personal Information & Usage Data

The data defined as personal data will be described by a HAT personal data use taxonomy. This is the definition of what data will be stored and collected by the HAT User and recorded by the HAT on the behaviour of the HAT User.

HAT INFORMATION POLICY 2 – Audit & Charging

The *personal data use taxonomy will be an auditable record* that will be visible to a *HAT User*. A HAT User will be able to see the usage of their HAT Data by HAT Service Providers. The HAT User will be able to access the audit record of their HAT Data. This includes a record of HAT-to-HAT Service transaction exchanges. A HAT Service Provider can record all HAT transactions collected or generated for a HAT User. A threshold can be set for how the HAT transaction may be chargeable by the HAT Service Provider.

HAT INFORMATION POLICY 3 – Visibility Of Data & Services

The HAT User will be able to control the visibility of HAT Personal Data to other HAT Users and/or HAT Service Providers. A HAT Service Provider may make their HAT Services visible to one or many HAT Users, but only HAT Personal Data that has received explicit consent from the HAT User owner of that data. This is to enable visibility to the *HAT Ecosystem* of HAT Services, HAT Devices and HAT Service Providers, HAT Applications and HAT Users within the conditions of the HAT User's consent to access and use their personal data.

HAT INFORMATION POLICY 4 – Personal Data Access Control

Definition of Access means "View only HAT Data"

A *person can control access to their personal HAT data*, controlling what is transmitted from or to other parties. This access control is provided by the HAT Service Provider to the HAT User over their HAT Data.

HAT INFORMATION POLICY 5 – Personal Data Usage Control

Definition of Usage means "able to add, update and change HAT Data"
A person can control their personal HAT Data use for a general or specific usage scenario for matching and general use. For example, the control of the use of HAT Personal Data that is for general sharing or private to access and use by HAT Service Providers, such as general interests and services. Or scenarios that involve specific personal data usage and choices for a HAT User, for example HAT User activity, user specific preferences, likes and dislikes to share with HAT Providers.

HAT INFORMATION POLICY 6 – Personal Authorisation Control

Definition of Authorisation means "able to set a permission level"
A person can control the access and use of their HAT Data by controlling the authorisation of its use. The *HAT Service Provider* will provide *Opt---in* and *Opt---out* choices for *HAT User authorisation permissions of their HAT Data*.

HAT INFORMATION POLICY 7 – Personal Data Release & Notification Control

Definition of Release means "able to control what is broadcast as notification"
A person can control the release of their HAT data to HAT Users and HAT Service Providers. The HAT Service Provider enables the HAT User to control the release of what HAT Personal Data is made available to HAT Service Providers. *Notifications* will be provided to the *HAT User* of when *HAT Data* has been accessed and used by the *Hat Service Provider* and between *HAT Services* transactions, including any security violations notifications of HAT Data that affect the HAT User. HAT Personal Data that is shared and used will be based on the *HAT User Authorised Permissions.*

HAT INFORMATION POLICY 8 – Personal Data Security

A HAT user is able to determine the security of their personal data by the HAT *Service Provider that is hosting their HAT Data*. This includes safeguards in managing HAT Personal Data such as firewalls and data encryption, physical access controls to HAT data centres, secure transmission and information access authorisation controls and monitoring, detection, notification, escalation and prevention of fraud and misuse of HAT Data.

HAT INFORMATION POLICY 9 – Personal Data Geolocation

All Personal HAT geolocation data tagging must be visible and controlled as an option

of anonymity by the Personal HAT User as part of the HAT *personal authorisation permissions.*

HAT INFORMATION POLICY 10 – Personal Data Removal

HAT Data would be removed after transactional use by the *HAT Service Provider*. The HAT Service Provider conducts data sanitation to ensure that *HAT User* data privacy is maintained after the data is used by HAT-ready Devices and HAT-ready Services. *HAT Data* that ceases to be hosted by a HAT Service Provider is removed from their HAT Hosting service and no longer accessible by that HAT Service Provider. HAT Data may only be retained based on compliance with local legal requirements.

5. HAT Certification Checklist

The HAT Foundation would certify HAT Platform Providers and HAT Service Providers (*device and service*) as HAT-Ready providers based on the evaluation of their compliance with HAT policies. The **HAT** Self-Certification **Checklist** entails the specific HAT Policy working procedures which would allow HAT Service Providers to conduct self-evaluation in terms of being HAT-Compliant, i.e. a HAT-ready Device and HAT-ready Service. The HAT Certification Checklist is as follows:

HAT CERTIFICATION CHECKLIST			Y/N
HAT POLICY 1		**DEFINITION OF PERSONAL INFORMATION & USAGE DATA**	**Y**
	1.1	The HAT Service Provider supports the current HAT Personal Data Taxonomy schema standard	y
	1.2	A HAT User can store their personal HAT Data and collect HAT Data	y
	1.3	A HAT User can collect their personal Data usage in their HAT Data	y
	1.4	A HAT User can create and manage their data as aggregated metadata "Bundle"	y
	1.5	A HAT Service Provider can record and set a threshold of HAT transactions per HAT User	y
HAT POLICY 2		**AUDIT & CHARGING**	**Y**
	2.1	The HAT Personal Data Taxonomy is auditable	y
	2.2	The use of HAT User Personal HAT Data is recorded and auditable	y
	2.3	All HAT Data transactions are auditable and reported to the HAT Foundation daily/weekly/monthly	y
	2.4	The use of Personal HAT Metadata "bundles" maybe auditable	y
	2.5	Ability to provide a report of all HAT transactions & notifications by HAT User and to the HAT Foundation	y
	2.6	Ability to set a threshold on the volume or type of HAT transaction that may or may not be charged to a Party	y
	2.7	Ability to set a threshold of HAT transactions that are reported by HAT User to the HAT Foundation	y
HAT POLICY 3		**VISIBILITY OF DATA & SERVICES**	**Y**
	3.1	The HAT Users registered to a HAT Provider	y

		are visible to the HAT Marketplace	
	3.2	The HAT User can control what data is visible to other participants in their HAT.	y
	3.3	The HAT Service Provider can control what HAT Services are visible to other parties.	y
	3.4	A HAT User can control what metadata "Bundles" is visible to other participants in their HAT.	y
HAT POLICY 4		**PERSONAL DATA ACCESS CONTROL**	**Y**
		Definition of Access means "View only HAT Data"	
	4.1	A HAT User can control the access to their personal HAT Data for requests from other parties to access that data	y
	4.2	A HAT User can control the access to their personal HAT Data in transmission of that data to other parties	y
	4.3	A HAT User can control the access of their personal HAT Data in receiving usage data from other parties into their HAT	y
	4.4	A HAT Service Provider can enable a HAT User to control access to their personal HAT	y
HAT POLICY 5		**PERSONAL DATA USAGE CONTROL**	**Y**
		Definition of Usage means "able to add, update and change HAT Data"	
	5.1	A HAT User can control a specific scenario of how their HAT Data is used in a life event in a specific location	y
	5.2	A HAT User can control how their HAT Data is used in a general event that may or may not be related to a location.	y
	5.3	A HAT User can control how their specific preferences for collecting usage data is received and stored in their personal HAT	y
HAT POLICY 6		**PERSONAL DATA AUTHORISATION CONTROL**	**Y**
		Definition of Authorisation means "able to set a permission level"	
	6.1	A HAT User can control the AUTHORISATION of access to their personal HAT Data	y
	6.2	A HAT User can authorise the Opt-in and Opt-out use of each HAT Data and HAT Metadata in their HAT	y
	6.3	A HAT Service Provider can enable a HAT User to set authorisation for each HAT	y

		Metadata "Bundles"	
	6.4	The ability to set a time limit when an authorisation is in force and expires between the HAT User and another party	y
HAT POLICY 7		**PERSONAL DATA RELEASE & NOTIFICATION CONTROL**	**Y**
		Definition of Release means "able to control what is broadcast as notification"	
	7.1	A HAT User can control what a HAT Service Provider releases of their HAT Data to another party.	y
	7.2	A HAT User can control the level of notifications alerts to their HAT Data, including access usages and authorisation	y
	7.3	A HAT Service Provider can provide notifications to specific HAT User or group of HAT Users	y
	7.4	A HAT Service Provider can provide notifications to a specific HAT Service Provider or group of HAT Service Providers	y
	7.5	A HAT Service Provider can provide HAT notifications to another party based on HAT User authorised permissions	y
	7.6	A HAT Service Provider can provide general notifications to another party	y
HAT POLICY 8		**PERSONAL DATA SECURITY**	**Y**
	8.1	A HAT User can view the HAT User Agreement they have with the HAT Service Provider	y
	8.2	A HAT Service Provider will display their Privacy Policy for HAT Users	y
	8.3	A HAT Service Provider will conform to local country legal security standards	y
	8.4	A HAT Service Provider will provide secure data management of HAT User data	y
	8.5	Content stored by the HAT User in their HAT Data is their Copyright and IP	y
HAT POLICY 9		**PERSONAL DATA GEOLOCATION**	**Y**
	9.1	A HAT User can control what HAT Data is collected by geolocation using a HAT-Ready Device or HAT-Ready Service	y
	9.2	A HAT Service Provider can record HAT Data and HAT usage data to a specific geolocation	y
	9.3	A HAT user can attribute a geolocation to a HAT Metadata Cabinet, for example, a	y

		lifestyle metadata view for a house location	
HAT POLICY 10		**PERSONAL DATA REMOVAL**	**Y**
	10.1	A HAT User can modify or delete their HAT Data from their HAT.	y
	10.2	A HAT User's data that has been changed or deleted can no longer be accessed by the HAT Service Provider or another party	y
	10.3	A HAT Service provider will only hold changed or deleted HAT Data for the duration that is legally required by local country laws	y
	10.4	A HAT User can port their HAT Data from one HAT Service Provider to another Service Provider	y
	10.5	A HAT User can delete their HAT Data from a HAT Service Provider.	y

6. HAT Certification Registration

What role are you Certified for?

HAT SERVICE PROVIDER	ROLE
HAT PLATFORM PROVIDER	Y
HAT APPLICATION PROVIDER	Y

Company Name:	
Contact Name:	
HATDeX Auditor:	
Date Certification Test	dd / mm /yy
HATDeX Certificati on Approved	dd / mm /yy
GUID Issue Date	dd / mm /yy
HAT Certification Valid to	dd / mm /yy
HATDeX Comments	

Compliance to HAT Information Policy checklist

HAT INFORMATION POLICY

CERTIFICATION	--- HAT INFORMATION POLICY	Y/N
HAT POLICY 1	DEFINITION OF PERSONAL INFORMATION & USAGE DATA	Y
HAT POLICY 2	AUDIT & CHARGING	Y
HAT POLICY 3	VISIBILITY OF DATA & SERVICES	Y
HAT POLICY 4	PERSONAL DATA ACCESS CONTROL	Y
HAT POLICY 5	PERSONAL DATA USAGE CONTROL	Y
HAT POLICY 6	PERSONAL DATA AUTHORIZATION CONTROL	Y
HAT POLICY 7	PERSONAL DATA RELEASE & NOTIFICATION CONTROL	Y
HAT POLICY 8	PERSONAL DATA SECURITY	Y
HAT POLICY 9	PERSONAL DATA GEOLOCATION	Y
HAT POLICY 10	PERSONAL DATA REMOVAL	Y

Key Glossary Terms

A list of terminology that is used in describing the Hub-of-All-Things ("The HAT")

Auditable	Ability to provide record of HAT transactions and parties' access to HAT Data
Geolocation	A physical location where data may be assigned to that location
GUID	Globally Unique Identifier to serve as the identification for a particular HAT in the ecosystem.
The HAT	A personal data platform developed by the *HAT Project* that allows a HAT user to acquire, store, transform, view, sell, rent, trade and use his or her personal data. Also known as the HAT Personal Data Platform (HATPDP)
HAT Application Provider (HAP)	A HAT Service Provider
HAT App Market	A marketplace of HAT-compliant applications where HAT users can buy or download to visualise, analyse or use their data
HAT CoP	**HAT Code(s) of Practice:** A set of practices to which all HAT Participants subscribe. It defines the HAT Code of Conduct of HAT Service Providers in order to certify and maintain compliance with the HAT Service and access to the HAT Marketplace
HAT Developer	Individuals who create HAT services who could be working for HAT Service Providers
HAT Data	Data from HAT-ready devices and services that the individual can use and is acquired into the user's own HAT
HAT Data "Bundle"	Aggregated or specific data grouped by an individual due to a contextualised use case. For example, a lifestyle bundle, a health bundle, a consumption bundle. Such bundles may contain data across multiple locations, people, time, and things.
HAT Data Usage	Data that is collected about the HAT User data

	usage, for example personal lifestyle and travel information, personal health or consumption data.
HAT Ecosystem	The community of all the individuals, firms and other organisations engaged in using the open source HAT technology, regulated by the HAT Foundation in compliance with the HAT CoP
HAT Foundation	The social enterprise grouping that will nurture and regulate the HAT ecosystem based on the open-sourced HAT technology
HAT Marketplace	An economic marketplace based on HAT Data and HAT Participants that is governed by a HAT Trust Framework
HAT (Exchange) Metadata	Metadata of a HAT Data Bundle, it contains the data points that have been grouped into a Bundle, but without the actual value of those data points
HAT Participants	Roles in the HAT Ecosystem. They include HAT Developers, HPPs, HAT Users, HAT Service Providers and the HAT Foundation
HATPDP	HAT Personal Data Platform; see the HAT for definition
HATPDP Provider (HPP)	An organisation that hosts users' HATs and supports a community of HAT developers by developing HAT services that improve the HATPDP capabilities
HAT-ready Device	A device that is able to send and/or receive data to/from the HAT in a way that is in compliance with the HAT CoP and certified by the HAT Foundation
HAT-ready Service	A service that is able to send and/or receive data to/from the HAT in a way that is compliant with the HAT CoP and certified by the HAT Foundation
HAT Service	A service that runs on the HAT at all levels of the technical architecture and complies with the HAT CoP
HAT Service Providers	Organisations who provide a HAT service on the HATPDP

HAT Traffic Data	Data about a personal HAT data, metadata, and usage data about HAT data and metadata
HAT Trust Framework	A set of principles and HAT CoP that are governed by the HAT Foundation
Life event	A specific event related to a person or company entity that may be related to one or more parties
Parties	A person or company entity that may or may not be a HAT Participant
Scenario	Ability to control how HAT Data is used in a specific geolocation or life event

Roles on the HAT Ecosystem

HAT User

Description: An individual who owns and uses HAT data and integrates data from their HAT---ready devices and services

Functions

1. Users register with a HATPDP Provider for a HAT
2. Users are given a unique HAT ID
3. Users authenticate their identity and access to their HATPDP Provider
4. Users acquire data from HAT device(s) and service(s) onto their HAT
5. User personalises their HAT through bundles or collections
6. Users lookup and check personal data on their HAT
7. Users can create an event and decide what HAT data is relevant to the event
8. Users can track their HAT data
9. Users can export their HAT data for sharing or to be used, bought or rented by third parties through the D3 system
10. User can see their list of D3s and transaction history
11. User can control their D3 system rules such as cancelling or modifying a D3

HAT App Developer (HAP)

Description: Developers who create HAT services

Functions

1. Develops HAT services that enable the sharing, buying, renting or operating of user applications on HAT data
2. Maintains working version of the HAT services
3. Provides regular software patches and updates to maintain the HAT services
4. Notifies the HPP when the HAT services are changed or deleted from use

HATPDP Provider (HPP)

Description: A platform provider that hosts users' HATs and supports a community of HAT developers by developing middleware capabilities

Functions

1. Defines the level that the HPP will operate the HAT database and service for a HAT user
2. Provides users with a HAT environment.
3. Ensures security of data on behalf of the HAT user
4. Ensures confidentiality of data through access control

5. Validates the service rules for event creation and data debit generation with the compliance of the user
6. Validates the data debit privacy rules
7. Validates data debit usage rules
8. Enforces the service rules and usage rules to enforce the privacy requirement

Hub-of-all-Things (HAT) Research Team (incorporating HARRIET)

Principal Investigator

Irene Ng Professor of Marketing and Service Systems, WMG, University of Warwick

Co-Investigators

Jon Crowcroft FRS, Marconi Professor of Communications Systems, Cambridge Computer Laboratory, University of Cambridge
Roger Maull Professor of Management Systems, Centre for Digital Economy, University of Surrey Business School
Glenn Parry Associate Professor in Strategy and Operations Management, Bristol Business School, University of the West of England
Tom Rodden Professor of Computing, University of Nottingham
Kimberley Scharf Professor of Economics, University of Warwick
Chris Speed Professor of Design Informatics, Edinburgh College of Art, University of Edinburgh
Ganna Pogrebna Associate Professor of Decision Science and Service Systems, WMG, University of Warwick (HARRIET)
Xiao Ma Senior Research Fellow, WMG, University of Warwick (HARRIET)

Funded Researchers

Andrius Aucinas University of Cambridge
Chris Barker University of Edinburgh
Roger Cliffe WMG, University of Warwick
Ewa Luger University of Nottingham
Anil Madhavapeddy University of Cambridge
Helen Oliver University of Cambridge
Laura Phillips University of Exeter
Peter Tolmie University of Nottingham
Susan Wakenshaw WMG, University of Warwick
Nabeel Shaikh WMG, University of Warwick
Martin Talbot WMG, University of Warwick

Affiliate Researchers

Saeed Aghaee University of Cambridge
Guo Lei National University of Singapore
Charith Perera The Australian National University
Nancy Olson WMG, University of Warwick
Mark Skilton University of Warwick

Industrial Advisory Board

Accenture	**GlaxoSmithKline**
ARUP	**HWP Consulting**
Autonect	**Mydex**
Bosch	**1248 Ltd**
DCS Europe	**Osram**
Dyson	**Sprue Aegis plc**
Enable Software	**Strand Hardware**
Fibaro	**Telefonica**

IAB Independent Chair: Paul Tasker

http://hubofallthings.com