Engineering a Market for Personal Data: The Hub-of-all-Things (HAT)
HAT Code of Practice on Personal Data
Version 1, November 2014

RCUK Digital Economy HAT Project
http://hubofallthings.org
Released 24 November, 2014
For more information, please contact sswmg@warwick.ac.uk

TABLE OF CONTENTS

HAT DATA COMPLIANCE ... 3

CODE OF PRACTICE ... 3

HAT CODE OF PRACTICE OBJECTIVES ... 4
HAT ROLES AND RESPONSIBILITIES ... 4
MANDATORY PRIVACY COMPLIANCE REQUIREMENTS FOR HAT ROLES ... 5
DESCRIPTION OF HAT PRIVACY COMPLIANCE POLICY FOUNDATIONS ... 5
HAT POLICY 1 - DATA USAGE ... 6
CODE OF PRACTICE PRINCIPLE 1 – HAT AUTHORISATION RULES ... 6
CODE OF PRACTICE PRINCIPLE 2 – HAT RELEASE RULES ... 6
CODE OF PRACTICE PRINCIPLE 3 – HAT PERSONAL POLICY RULES ... 7
HAT POLICY 2 - DATA USE TAXONOMY ... 7
CODE OF PRACTICE PRINCIPLE 4 – HAT PERSONAL DATA USE TAXONOMY ... 7
CODE OF PRACTICE PRINCIPLE 5 – HAT AUDITABLE RECORD ... 8
CODE OF PRACTICE PRINCIPLE 6 – HAT TRUST FRAMEWORK ... 8
HAT POLICY 3 - HAT PROVENANCE ... 9
CODE OF PRACTICE PRINCIPLE 7 – HAT LOCATION USAGE POLICY ... 9
CODE OF PRACTICE PRINCIPLE 8 – HAT SCENARIO USAGE POLICY ... 9
CODE OF PRACTICE PRINCIPLE 9 – HAT EVENT ALERT POLICY ... 10
CODE OF PRACTICE PRINCIPLE 10 – HAT TRANSMISSION CONTROL USAGE POLICY ... 10
HAT POLICY 5 - HAT USAGE POLICY ENFORCEMENT ... 11
CODE OF PRACTICE PRINCIPLE 11 – HAT DATA POLICY BINDING LIFECYCLE ... 11
CODE OF PRACTICE PRINCIPLE 12 – HAT DATA NON-COMPLIANCE DETECTION ... 11
HAT POLICY 6 – HAT TRUST IDENTITY MANAGEMENT ... 12
CODE OF PRACTICE PRINCIPLE 13 – HAT TRUST POLICY MANAGEMENT ... 12
CODE OF PRACTICE PRINCIPLE 14 – HAT IDENTITY MANAGEMENT ... 12
CODE OF PRACTICE PRINCIPLE 15 – HAT AUTHENTICATION MANAGEMENT ... 13
HAT POLICY 7 – HAT ACCESS CONTROL ... 13
CODE OF PRACTICE PRINCIPLE 16 – HAT ACCESS APPROVAL ... 13
CODE OF PRACTICE PRINCIPLE 17 – HAT DATA GEOLOCATION TAGGING ... 14
CODE OF PRACTICE PRINCIPLE 18 – HAT DATA DEVICE DISCOVERABILITY ... 14
HAT POLICY 8 – HAT SECURITY ... 15
CODE OF PRACTICE PRINCIPLE 19 – HAT SECURITY MONITORING & PROTECTION ... 15
CODE OF PRACTICE PRINCIPLE 20 – HAT E-DISCOVERY ... 15

CODE OF PRACTICE PRINCIPLE 21 – HAT DATA ENCRYPTON *16*

CODE OF PRACTICE PRINCIPLE 22 – HAT DATA STORAGE *16*

CODE OF PRACTICE PRINCIPLE 23 – HAT DATA TRANSMISSION *16*

APPENDIX 1........18

HAT PERSONAL PRIVACY POLICIES *18*

APPENDIX 2........21

NOTES ON HAT DEFINITIONS *21*

REFERENCES........22

GLOSSARY OF TERMS 23

Hub-of-all-Things (HAT) Research Team (incorporating the HARRIET team)........27

The Investigators........ 27

Principal Investigator *27*

Co-Investigators *27*

The Researchers........ 27

Funded Researchers *27*

Affiliate Researchers *28*

Industry Advisory Board........ 28

HAT DATA COMPLIANCE

CODE OF PRACTICE

This CODE OF PRACTICE aims to articulate the privacy, security and confidentiality compliance principles and working practices of data for all ROLES involved in the HAT ecosystem.

These principles are developed based on the HAT PROJECT/FOUNDATION user-centered approach to privacy, which could be implemented through an interoperable metadata-based architecture.

A CODE OF PRACTICE IS A SET OF PROCEDURES THAT DEFINE THE RESPONSIBLE ACTIONS AND OUTCOMES FOR ALL ROLES INVOLVED IN A BUSINESS PROCEDURE.

A CODE OF PRACTICE IS AN IMPLEMENTATION OF A SET OF POLICIES DEFINED BY AN ORGANISATION ENTITY, IN THIS CASE THE HAT PROJECT/FOUNDATION, REPRESENTING THE OPERATIONAL STRATEGY AND PROCEDURES NECESSARY TO SUCCESSFULLY IMPLEMENT THAT STRATEGY.

THIS HAT CODE OF PRACTICE DOCUMENT IS DEFINED BY HAT DATA COMPLIANCE POLICIES AND THE HAT CODE OF PRACTICE PRINCIPLES TO IMPLEMENT THESE POLICIES.

HAT CODE OF PRACTICE OBJECTIVES

The objective of a HAT CODE OF PRACTICE is to set up the principles, practices and a regulatory framework around the management of data within the HAT ecosystem for the purpose of maintaining privacy, confidentiality, and security of HAT data whilst incentivising innovation and creating new opportunities for services around personal data.

This document specifically covers TWO procedures:

1. HAT ROLES AND RESPONSIBILITIES
    a. The Code of Practice for roles and responsibilities assigned to specific ENTITIES involved directly with the management of data on HATPDP and HAT-ready device or service.

2. MANDATORY PRIVACY COMPLIANCE REQUIREMENTS FOR HAT ROLES
    a. The principles that must be followed by each HAT role, describing the primary activities that are defined as requirements for a HAT process compliance.

HAT ROLES AND RESPONSIBILITIES

This CODE OF PRACTICE applies to the following HAT roles involved in a HAT SERVICE.

The specific definitions of these roles and a HAT service can be found in the HAT GLOSSARY.

HAT ROLE 1	HAT USER
HAT ROLE 2	HAT DEVELOPER
HAT ROLE 3	HAT PLATFORM PROVIDER (HPP)
HAT ROLE 4	HAT PROJECT/FOUNDATION

MANDATORY PRIVACY COMPLIANCE REQUIREMENTS FOR HAT ROLES

EIGHT POLICIES define the HAT FOUNDATION definition of compliancy of a HAT service.

A description of the policy foundations can be found in the appendix of this document.

HAT POLICY 1	HAT DATA USAGE
HAT POLICY 2	HAT DATA USAGE TAXONOMY
HAT POLICY 3	HAT PROVIDENCE
HAT POLICY 4	HAT POLICY ENFORCEMENT MANAGEMENT
HAT POLICY 5	HAT USAGE POLICY MANAGEMENT
HAT POLICY 6	HAT TRUST IDENTITY MANAGEMENT
HAT POLICY 7	HAT ACCESS CONTROL
HAT POLICY 8	HAT SECURITY

DESCRIPTION OF HAT PRIVACY COMPLIANCE POLICY FOUNDATIONS

A Personal Data Management System ("the HAT") is a personal single tenant ("the individual self") technology system that is fully individual self-service, (non-technical user friendly and requiring no technical skills) to enable an individual to define a full set of "meta-data" defining as a specific set of personal data, personal preferences, personal behaviour events. The HAT allows individuals to share the right information (quality and quantity), with the right people, in the right situations for the right purposes and gain the benefits. In terms of information privacy, we take a user-centered approach and regard privacy as a dialectic and dynamic boundary regulation process between three entities such as the data subject (self), personal information/data (premise), and the other (people, firm etc). In order to implement HAT privacy, we suggest taking into account social (situations), technical (data architecture) and regulatory (policy) (Nguyen, et al, 2013). This approach focuses on the development of policies, which includes user-specified permission, corporate policies, and applicable regulations. The specification of user permissions and policies and regulations would govern how data can be used within shared across-trust boundaries. These permissions and policies would be negotiated among multiple parties with claims on the data. THE HAT FOUNDATION APPROACH IS that user permissions and policies would represent the factors described above INCLUDING (1) situations (2) boundaries (3) contextual integrity, (4) applicable regulation for individual data.

HAT POLICY 1 - DATA USAGE

CODE OF PRACTICE PRINCIPLE 1 – HAT AUTHORISATION RULES

A person can define the authorisation rules of their personal HAT data in the HAT for any or specific usage scenario. Note: a usage scenario authorisation is the level of data collection and visibility of personal data in a given scenario. For example, “in the shower” is a usage scenario, which you want to be partially authorised to use this data. This may be from “private – not available,” to specific data on water usage and time in and out of the shower, “soap and shampoo product usage.”

SPECIFIC ROLES & RESPONSIBILITIES

- HAT USER
  - The HAT User can define and control authorisation rules
- HAT DEVELOPER
  - The Developer of the HAT software application must enable personal HAT data to have authorisation rules
- HAT PLATFORM PROVIDER (HPP)
  - The HAT Provider must manage the HAT Service to comply with the HAT User authorisation rules
- HAT PROJECT/FOUNDATION
  - The HAT Foundation defines the required authorisation rules in the HAT Data specification.

CODE OF PRACTICE PRINCIPLE 2 – HAT RELEASE RULES

A person controls the release rules (conditional mandatory rules defined by the person) of personal HAT data to any or specific 3rd party, that is not the HAT user. Note: this is a specific release rule to any or specific 3rd party. This controls what usage scenario information is allowed to be shared with any or specific 3rd parties.

SPECIFIC ROLES & RESPONSIBILITIES

- HAT USER
  - The HAT User can define and control their HAT Data release rules
- HAT DEVELOPER
  - The HAT Developer of the HAT software app must enable personal HAT data to have HAT Data release rules
- HAT PROVIDER
  - The HAT Provider must manage the HAT Service to comply with the HAT User personal HAT Data release rules
- HAT FOUNDATION
  - The HAT Foundation defines the required personal HAT Data release rules in the HAT Data specification

CODE OF PRACTICE PRINCIPLE 3 – HAT PERSONAL POLICY RULES

A person can define specific policy rules for use of their personal HAT data. These include access and usage control rules. This relates to how the HAT personal data is customised by the HAT user in their Personal HAT.

SPECIFIC ROLES & RESPONSIBILITIES

- HAT USER
  - The HAT User can define and control their HAT Data customisation rules stating how this data is accessed, and usage recorded.
- HAT DEVELOPER
  - The HAT Developer of the HAT software app must enable personal HAT data to have HAT Data customisation rules, selecting the types of HAT type they wish to use in the HAT software application service.
- HAT PROVIDER
  - The HAT Provider must manage the HAT Service to comply with the HAT User personal HAT Data customisation rules
- HAT FOUNDATION
  - The HAT Foundation defines the required personal HAT Data customisation rules in the HAT Data specification.

HAT POLICY 2 - DATA USE TAXONOMY

CODE OF PRACTICE PRINCIPLE 4 – HAT PERSONAL DATA USE TAXONOMY

The HAT User data defined as personal data will be described by a personal data use taxonomy. Note: a personal data use taxonomy refers to the specific personal data and metadata (data describing personal data and its use) recorded and held in the HAT.

SPECIFIC ROLES & RESPONSIBILITIES

- HAT USER
  - The HAT User can access and see all their HAT data and metadata defined in their Personal HAT
- HAT DEVELOPER
  - The HAT Developer of the HAT software app must enable personal HAT data to see and access all HAT data and Metadata used to define their personal HAT.
- HAT PROVIDER
  - The HAT Provider must manage the HAT Service to comply with the HAT user-defined rules for the usage of personal HAT Data and Metadata used to define their personal HAT
- HAT FOUNDATION
  - The HAT Foundation defines the required Personal HAT Data and metadata taxonomy schema in the HAT Data specification.

CODE OF PRACTICE PRINCIPLE 5 – HAT AUDITABLE RECORD

The HAT User personal data use taxonomy will be an auditable record that can be seen and accessed by the HAT User.

SPECIFIC ROLES & RESPONSIBILITIES

- HAT USER
  - The HAT User must be able to have an audit record of their HAT data usage. They must be able to access and see the audit record.
- HAT DEVELOPER
  - The HAT Developer of the HAT software app must enable personal HAT data to be auditable.
- HAT PROVIDER
  - The HAT Provider must manage the HAT Service to comply with the HAT user-defined rules of usage of personal HAT Data by proving an audit record of all usage of their personal HAT. This must be accessible to the HAT user.
- HAT FOUNDATION
  - The HAT Foundation defines the required Personal HAT audit checks based on the HAT Data specification

CODE OF PRACTICE PRINCIPLE 6 – HAT TRUST FRAMEWORK

The HAT User can define rules for all 3rd parties that can access their personal HAT Data. This is called the HAT TRUST FRAMEWORK. The HAT trust framework describes for each HAT User their Personal interoperable data-use taxonomy.

SPECIFIC ROLES & RESPONSIBILITIES

- HAT USER
  - The HAT User must be able to define their HAT trust rules for all 3rd party access to their personal HAT.
- HAT DEVELOPER
  - The HAT Developer of the HAT software app must enable the APP to comply with HAT user-defined rules for the usage of HAT Data and trust rules for HAT data defined by the personal HAT user.
- HAT PROVIDER
  - The HAT Provider must manage the HAT Service to comply with HAT user-defined rules of usage of personal HAT Data by supporting the trust rules for their personal HAT. This must be defined by the HAT User.
- HAT FOUNDATION
  - The HAT Foundation defines the required personal HAT trust framework schema based on the HAT Data specification

HAT POLICY 3 - HAT PROVENANCE

CODE OF PRACTICE PRINCIPLE 7 – HAT LOCATION USAGE POLICY

The HAT User can define their HAT Policies to be changeable to situations and contexts.

SPECIFIC ROLES & RESPONSIBILITIES

- HAT USER
  - The HAT User must be able to define their HAT Data location and context usage rules.
- HAT DEVELOPER
  - The HAT Developer of the HAT software app must enable HAT users to define the usage of HAT Data location and context usage rules.
- HAT PROVIDER
  - The HAT Provider must manage the HAT Service to comply with the HAT user-defined rules of usage of personal HAT Data by supporting the HAT Data location and context usage rules. This must be defined by the HAT User.
- HAT FOUNDATION
  - The HAT Foundation defines the required personal HAT Data location and context usage rules based on the HAT Data specification.

CODE OF PRACTICE PRINCIPLE 8 – HAT SCENARIO USAGE POLICY

The HAT User can control their personal HAT Data use for any or specific usage scenario. A scenario relates to an event that may act on using a HAT Service and HAT Data that can impact a HAT User.

SPECIFIC ROLES & RESPONSIBILITIES

- HAT USER
  - The HAT User must be able to define their HAT Data usage scenario.
- HAT DEVELOPER
  - The HAT Developer of the HAT software app must enable HAT users to define the HAT Data usage scenario.
- HAT PROVIDER
  - The HAT Provider must manage the HAT Service to comply with the HAT user-defined rules of usage of personal HAT Data by supporting the HAT Data usage scenario. This must be defined by the HAT User.
- HAT FOUNDATION
  - The HAT Foundation defines the required personal HAT Data usage scenario rules based on the HAT Data specification.

CODE OF PRACTICE PRINCIPLE 9 – HAT EVENT ALERT POLICY

The HAT User must be able to have any use of their personal HAT Data recorded and made visible through an event alert that may be communicated immediately or by some personal rule of the identity of the entity accessing the personal HAT Data.

SPECIFIC ROLES & RESPONSIBILITIES

- HAT USER
  - The HAT User must be able to define their HAT Data event alert rules.
- HAT DEVELOPER
  - The HAT Developer of the HAT software app must enable HAT users to define the usage rules for HAT Data event alert rules.
- HAT PROVIDER
  - The HAT Provider must manage the HAT Service to comply with the user-defined rules for the usage of HAT personal Data by supporting the HAT Data event alert rules. This must be defined by the HAT User.
- HAT FOUNDATION
  - The HAT Foundation defines the required Personal HAT Data event alert rules based on the HAT Data specification .

CODE OF PRACTICE PRINCIPLE 10 – HAT TRANSMISSION CONTROL USAGE POLICY

A HAT User can control personal HAT Data access to or from transmission from their HAT. Transmission rules relate to HAT OUTBOUND API activity and the ability to control permissions to send HAT Data.

SPECIFIC ROLES & RESPONSIBILITIES

- HAT USER
  - The HAT User must be able to define their HAT Data transmission rules.
- HAT DEVELOPER
  - The HAT Developer of the HAT software app must enable personal HAT Data to define and use HAT Data transmission rules.
- HAT PROVIDER
  - The HAT Provider must manage the HAT Service to comply with the HAT User-defined rules for the usage of personal HAT Data by supporting the HAT Data transmission rules. This must be defined by the HAT User.
- HAT FOUNDATION
  - The HAT Foundation defines the required Personal HAT Data transmission rules based on the HAT Data specification.

HAT POLICY 5 - HAT USAGE POLICY ENFORCEMENT

CODE OF PRACTICE PRINCIPLE 11 – HAT DATA POLICY BINDING LIFECYCLE

HAT User Policies are bounded to their HAT Data during the whole data life cycle for data held in their HAT.

SPECIFIC ROLES & RESPONSIBILITIES

- HAT USER
  - The HAT User must be able to define their HAT Data rules binding to the usage of HAT Data.
- HAT DEVELOPER
  - The HAT Developer of the HAT software app must enable personal HAT Data to define and use HAT Data rules binding to the usage of HAT Data.
- HAT PROVIDER
  - The HAT Provider must manage the HAT Service to comply with the HAT User-defined rules for the usage of personal HAT Data by supporting the HAT Data rules binding to the usage of HAT Data. This must be defined by the HAT User.
- HAT FOUNDATION
  - The HAT Foundation defines the required Personal HAT Data rules binding to the usage of HAT Data based on the HAT Data specification.

CODE OF PRACTICE PRINCIPLE 12 – HAT DATA NON-COMPLIANCE DETECTION

HAT Provider Technologies must protect a HAT User, for example, a “honey-pot-system” would be installed for the enforcement of the policies.

SPECIFIC ROLES & RESPONSIBILITIES

- HAT USER
  - The HAT User must be able to see and access the status of their HAT Data usage non-compliance base on their HAT usage rules.
- HAT DEVELOPER
  - The HAT Developer of the HAT software app must enable personal HAT Data to be monitored and assessed for non-compliance usage.
- HAT PROVIDER
  - The HAT Provider must provide a HAT Service to monitor personal HAT Data usage non-compliance. This must be visible and accessible to the HAT User. Any non-compliance should be alerted to the HAT User.
- HAT FOUNDATION
  - The HAT Foundation defines the required Personal HAT Data monitoring compliance based on the HAT Data specification.

HAT POLICY 6 – HAT TRUST IDENTITY MANAGEMENT

CODE OF PRACTICE PRINCIPLE 13 – HAT TRUST POLICY MANAGEMENT

A HAT User can view and access a HAT policy-management service from their HAT Provider. The HAT Policy management service is used to distribute policies to enable all the authorised 3rd party HAT parties to get the latest version of the stored policies.

SPECIFIC ROLES & RESPONSIBILITIES

- HAT USER
  - The HAT User must be able to see and access how all HAT policies versions are complied with by 3rd parties that may use their personal HAT.
- HAT DEVELOPER
  - The HAT Developer of the HAT software app must enable identification of all versions of HAT policies that it complies with.
- HAT PROVIDER
  - The HAT Provider must provide a HAT Service to monitor personal HAT Data usage non-compliance. This must be visible and accessible to the HAT User. Any non-compliance should be alerted to the HAT User.
- HAT FOUNDATION
  - The HAT Foundation defines the required Personal HAT Policy registration rules based on the HAT Data specification (ref).

CODE OF PRACTICE PRINCIPLE 14 – HAT IDENTITY MANAGEMENT

A HAT User must be provided with a personal HAT system that has an identity access management (IAM) system that controls the verification of any entity (the individual owner of their HAT or any 3rd party) to access control authentication and authorisation (A&A) to any part of the personal HAT data. (The HAT has its own A & A system).

SPECIFIC ROLES & RESPONSIBILITIES

- HAT USER
  - The HAT User must be able to use an IAM system to control the access authorisation of their personal HAT
- HAT DEVELOPER
  - The HAT Developer of the HAT software app must support an IAM system to control the access authorisation to use the HAT Service.
- HAT PROVIDER
  - The HAT Provider must provide an IAM system to control HAT access authorisation.
- HAT FOUNDATION
  - The HAT Foundation defines the required Personal HAT identity management rules based on the HAT Data specification.

CODE OF PRACTICE PRINCIPLE 15 – HAT AUTHENTICATION MANAGEMENT

A HAT User must be able to see and access through their HAT Provider, an identity service to allow all parties to register and authenticate to use data across the multiple trust framework.

SPECIFIC ROLES & RESPONSIBILITIES

- HAT USER
  - The HAT User must be able to use the register of trust to control the access registration and authorisation access to their personal HAT
- HAT DEVELOPER
  - The HAT Developer of the HAT software app must support a trust access authorisation to use the HAT Service.
- HAT PROVIDER
  - The HAT Provider must provide a trust management system to control all parties' access authorisation to a personal HAT.
- HAT FOUNDATION
  - The HAT Foundation defines the required Personal HAT trust framework rules based on the HAT Data specification (ref)

HAT POLICY 7 – HAT ACCESS CONTROL

CODE OF PRACTICE PRINCIPLE 16 – HAT ACCESS APPROVAL

A HAT User has primary & exclusive control over access to their personal HAT Data. A personal HAT provider must get approval from the personal HAT User.

SPECIFIC ROLES & RESPONSIBILITIES

- HAT USER
  - The HAT User must be able to grant approvals for access to their personal HAT
- HAT DEVELOPER
  - The HAT Developer of the HAT software app must support an approvals process to access and use the HAT Service.
- HAT PROVIDER
  - The HAT Provider must provide an approvals system to control all parties' access authorisation to a personal HAT.
- HAT FOUNDATION
  - The HAT Foundation defines the required Personal HAT approvals rules based on the HAT Data specification.

CODE OF PRACTICE PRINCIPLE 17 – HAT DATA GEOLOCATION TAGGING

All personal HAT Data geolocation data tagging must be visible and controlled as an option of anonymity by the personal HAT User.

SPECIFIC ROLEs & RESPONSIBILITIES

- HAT USER
  - The HAT User must be able to geotag and control the tagging and access of this data in their personal HAT.
- HAT DEVELOPER
  - The HAT Developer of the HAT software app must support geotagging of data that use the HAT Service. This must also support options to block or remove geotagging as an option controlled by the HAT User.
- HAT PROVIDER
  - The HAT Provider must provide a geotagging system to control all parties' access authorization to a personal HAT. This must also support options to block or remove geotagging as an option controlled by the HAT user.
- HAT FOUNDATION
  - The HAT Foundation defines the required Personal HAT geotagging option rules based on the HAT Data specification.

CODE OF PRACTICE PRINCIPLE 18 – HAT DATA DEVICE DISCOVERABILITY

Specific HAT access control rules for example device discoverability and access to HAT Data. For example: 1. Bluetooth, 2. Wi-Fi shared 3. Others.

SPECIFIC ROLES & RESPONSIBILITIES

- HAT USER
  - The HAT User must be able to define and control device discoverability rules of their personal HAT
- HAT DEVELOPER
  - The HAT Developer of the HAT software app must support device discoverability rules that use the HAT Service.
- HAT PROVIDER
  - The HAT Provider must provide device discoverability rules service to control all parties' access authorisation to a personal HAT.
- HAT FOUNDATION
  - The HAT Foundation defines the required Personal HAT device discoverability rules based on the HAT Data specification.

HAT POLICY 8 – HAT SECURITY

CODE OF PRACTICE PRINCIPLE 19 – HAT SECURITY MONITORING & PROTECTION

A personal HAT Platform Provider provides intrusion monitoring and specifies their defence to unauthorised access to a personal HAT.

SPECIFIC ROLES & RESPONSIBILITIES

- HAT USER
  - The HAT User must be able to access and see alerts from intrusion monitoring and alerts to their personal HAT.
- HAT DEVELOPER
  - The HAT Developer of the HAT software app must support intrusion monitoring and response that use the HAT Service.
- HAT PROVIDER
  - The HAT Provider must provide intrusion monitoring and response service to control all parties' access authorisation to a personal HAT.
- HAT FOUNDATION
  - The HAT Foundation defines the required Personal HAT intrusion monitoring and response rules based on the HAT Data specification.

CODE OF PRACTICE PRINCIPLE 20 – HAT E-DISCOVERY

All personal HAT Data entries will be logged and archived to support e-discovery rules. A personal HAT Data must be archived and reproducible for a specific period by the HAT Provider based on the e-Discovery conditions' specified rules. (A rule may be that all historical HAT data is archived in perpetuity or destroyed after a given time).

SPECIFIC ROLES & RESPONSIBILITIES

- HAT USER
  - The HAT User must be able to be access and see e-Discovery audit to their personal HAT.
- HAT DEVELOPER
  - The HAT Developer of the HAT software app must support e-Discovery audit that use the HAT Service.
- HAT PROVIDER
  - The HAT Provider must provide an e-Discovery service to control all parties' access and archiving of e-Discovery data of a personal HAT.
- HAT FOUNDATION
  - The HAT Foundation defines the required Personal HAT e-Discovery archive rules based on the HAT Data specification.

CODE OF PRACTICE PRINCIPLE 21 – HAT DATA ENCRYPTON

Principle-specific HAT encryption rules are specific technology standards used to encrypt HAT Data.

SPECIFIC ROLES & RESPONSIBILITIES

- HAT USER
  - The HAT User must be able to encrypt their personal HAT.
- HAT DEVELOPER
  - The HAT Developer of the HAT software app must support data encryption that use the HAT Service.
- HAT PROVIDER
  - The HAT Provider must provide a data encryption service of a personal HAT.
- HAT FOUNDATION
  - The HAT Foundation defines the required Personal HAT data encryption rules based on the HAT Data specification.

CODE OF PRACTICE PRINCIPLE 22 – HAT DATA STORAGE

HAT data-at-rest stored in the HAT, for example: symmetric private keys; asymmetric public keys; other.

SPECIFIC ROLES & RESPONSIBILITIES

- HAT USER
  - The HAT User must be able to control security access to their personal HAT.
- HAT DEVELOPER
  - The HAT Developer of the HAT software app must support security access service that use the HAT Service.
- HAT PROVIDER
  - The HAT Provider must provide a security access service of a personal HAT.
- HAT FOUNDATION
  - The HAT Foundation defines the required Personal HAT security access rules based on the HAT Data specification (ref).

CODE OF PRACTICE PRINCIPLE 23 – HAT DATA TRANSMISSION

HAT data transmitted to and from the HAT, for example: transport transfer protocol. For example: http-s; transport tunnel protocol – VPN; others.

SPECIFIC ROLES & RESPONSIBILITIES

- HAT USER
  - The HAT User must be able to use secure transmission protocols for their personal HAT.
- HAT DEVELOPER
  - The HAT Developer of the HAT software app must support secure transmission service that uses the HAT Service.
- HAT PROVIDER
  - The HAT Provider must provide a secure transmission service of a personal HAT.
- HAT FOUNDATION
  - The HAT Foundation defines the required Personal HAT secure transmission rules based on the HAT Data specification (ref).

APPENDIX 1

HAT PERSONAL PRIVACY POLICIES

Description of Hat Usage Policy And Provence Policy 1 Foundations

Because the policies attached to the data must represent the interest of all parties, it is possible to have multiple policies of each type attached to data. These policies would include: (1) Data collector policy; (2) User-specified permissions; (3) Global user policies; (4) Regulatory and jurisdictional policies: these specify requirements that depend on where data is collected and used. For example, there may be requirements to attach policies to data collected from minors in a specific country/origin; (5) Legal documents: these are entered into with the data collector and other third parties and govern the relationships between them. For example, an agreement may specify the frequency with which a data collector must refresh data they obtain from a third party (Nguyen et al, 2013).

Description of Hat Data Use Taxonomy Policy 2 Foundations

To ensure that data is used in accordance with policies bound to it, a data-use taxonomy must be defined and understood by parties within a given trust framework. The taxonomy should describe common access, sharing, use, and disposal patterns. For example, a simple taxonomy could include (1) who can data be shared with? (2) What use is the data intended for? (3) How long can the data be kept? (4) Where, geographically can the data be transferred? (5) How identifiable is the data subject and other parties? (Nguyen et al, 2013, p.238). It needs to provide a way to make data-use taxonomy interoperable. HAT provides a common way to describe uses that are attached to the data. In a trust framework, all parties can map their own data use taxonomy to an interoperable taxonomy through common interface and schemas.

Description of Hat Provenance Policy 3 Foundations

Provenance describes the origins of the data such as time, location, data-collector, and data-collector information; it can also specify whether the data was actively collected, generated, or inferred/ …Provenance can also include the same information about the policy/policies bound to the data. Provenance could also possibly track where data originated as it flows in an ecosystem. Provenance can also be used to track data controllers during forward transfers to show the chain of custody of the data, and also show additional policies that are attached to the data. (Nguyen et al, 2013, p.237).

Description of Hat Policy Enforcement 4 Foundations

Binding policy to data can help make the obligations and requirements for data use clear. For less sensitive data, communicating the obligations may in itself be sufficient. For more sensitive data, parties may want more assurance and better security so that only trusted parties can access and use it and there is no ambiguity about requirements for use.

Because the metadata includes a pointer to a gatekeeper, which can provide authoritative information about the policies that are bound to it, we can also enable additional functionality depending on the sensitivity of the data. When an entity wants to use data, it

goes to the gatekeeper to evaluate the latest policy. For less sensitive data, that may satisfy the requirement for the data controller. For more sensitive data, this may be the first step in a longer authentication and authorisation process. The data controller may require that the requestor provide additional claims from a trusted claim provider, such as the verified identity of the requestor and the health of their system. The data controller can also choose to encrypt data and only permit an exchange of keys when the requester has met certain criteria.

In addition to the technical ways to enforce policies, a trust framework or a jurisdiction may also define requirements about how policies are enforced. It could potentially be a legal rule that policy bound to data is respected, and violating such policies could have civil or criminal penalties. (Nguyen et al, 2013, p.238).

Description of Hat Policy Management 5 Foundations

A policy management services could provide authoritative locations where parties can get the latest version of stored policies. A policy management service would distribute policies among multiple servers and be replicated across geographic areas to improve latency and robustness of policy lookups.

Description of Hat Trust Identity Management Policy 6 Foundations

Identity services, which allow parties to register and authenticate to use data across multiple trust frameworks, also make other aspects of the architecture interoperable by connecting data and actions to authenticated parties across the ecosystem (Nguyen et al 2013, p.239).

Description of Hat Access Control Policy 7 Foundations

Confidentiality concerns the externalisation of restricted but accurate information to a specific entity. It entails the restricted release of information under an agreement which entails the limits, the condition etc. It can be suggested that a user-centred approach to privacy can be employed to achieve the confidentiality described above. Confidentiality involves the ‘agreement’ describing the limits, the conditions under which the data can be externalised by the data controller to a specific entity. The data-use taxonomy can describe common access, sharing, use and disposal patterns, which can be understood by parties within a trust framework. Confidentiality also concerns the limits, conditions in order to externalise the data in a restricted and accurate manner. In order to specify the conditions and limits, the situations (normative and individual specific) need to be considered in order to derive the information norms for the contextual integrity of the data transmissions in the context. Thus, the HAT providers need to develop the information norms and data transmission policies. These policies need to be managed and provided in an authorised location. Confidentiality entails the release of the data to a specific entity. The eligibility to access more sensitive data can be determined in a longer authentication and authorisation process. The data controller may require the requestor provide additional claims from a trusted claim provider, such as the verified identity of the requestor and the health of their system. The data controller can also choose to encrypt data and only permit an exchange of keys when the requester has met certain criteria.

Description OF HAT Security Policy 8 Foundations

Security concerns the protection of data including (1) integrity that assures information is not altered during transit and storage; (2) access: authentication that addresses the verification of a user's identity and eligibility to data access; (3) and confidentiality that requires data use is confined to authorised purposes by authorised people. Security of data could be against various risks, such as risks of data being accessed or modified by unauthorised persons in storage and during transmission.

In order to ensure that the data is accessed and used by the authorized purposes, the user-policy would be bound to the data throughout the data-use lifecycle. Policies that are bound to the data would be included by reference, with pointers to the most recent policy. Policies need to be changeable with the changing relationships and contexts. The entity is able to and then obligated to check the latest policies version and respect that specific version. Reconciliation capabilities and processes must be part of the trust framework to ensure policies bound to the data can be respected and reconciled. Thus, the HAT provider needs to enable the stakeholders of HAT to access, update, reconcile and be obliged by the latest policies of use of the data to guarantee that the data is accessed and used for the authorised purposes.

In order to ensure that the data is accessed by the authorised person, there will be mechanisms to conduct the identity check through authorisation and authentication, and encryption. In addition, there are some access control model (such as role-based access control model) and information flow control measures to control the access to the data for security, such as: (1) end-to-end security policies; (2) multi-level security models; (3) end-to-end confidentiality policies; and (4) mandatory access control models. Logs are the way to track the flow of information. Logs can be used for both individuals and for the servers. On the individual side, logs that are summarised in a compact form make it easier for the individuals to understand who is accessing what data. On the server side, logs make it easy for the HAT providers to audit their activities to ensure that they are handling the individuals' data properly. On both sides, logs also make it possible to apply machine learning techniques to detect unusual access patterns that might indicate abuses of someone's personal information (Landay, et al, 2004).

In order to control the information flow in the metadata-based architecture, the use-data taxonomy will cover these issues (such as whether it should be forwarded to others and how long it should be retained), and restrictions (based on identity, location etc) can be bounded with the data throughout the data-use lifecycle. In addition, these preferences can be tagged, which can be used as fingerprint to help with the tracking and auditing as well.

It can be suggested that HAT providers would develop a HAT security infrastructure by employing these measures for different types of data to ensure that the appropriate level of security could be achieved for them.

APPENDIX 2

NOTES ON HAT DEFINITIONS

1. Defined by legal age and verified by registered National Insurance (NI) Number. (For example, in the UK all applications for finance typically require proof or ability to work in the country. NI registration requires passport identity registration to confirm person is a resident in the country. Adults may use the system over the age of 18. A minor is classified by the UN Convention on the Rights of the Child, ratified by the UK government in 1991 which states that a child "means every human being below the age of eighteen years unless, under the law applicable to the child, majority is attained earlier" (Article 1, Convention on the Rights of the Child, 1989).
2. The Tenancy of a HAT is defined to an individual in their country of residence and bound by those laws. That HAT is also hosted and resident to that country. A citizen from another country may access their HAT from another country when abroad in another country of current residency. PATRIOT and Subpoena laws may be enacted on data not resident in the country of origin.
3. "Personal data" and "Personal metadata" is defined as unique data specific to the individual whereas metadata is specific data describing the personal data. An example of this is my name "John Smith", "age 25" who lives in "Basingstoke, UK" and metadata, "gender, Male", "age range", and "Residence". Specific characteristics of a person's events, behaviour or preferences that are attributable to the individual but are not mutually exclusive (can be a preference of behaviour that may be common to others). Examples of this could be "viewed movie "Avatar" on living room from 14.50 to 16.35pm on Sept 25, 2014" and metadata "viewing habits", "channel choice", "Device viewer Tablet", "location", "time entered room, door opened", "time left room, door opened, closed", "activity time and date".

REFERENCES

Barth, A., Datta, A., Mitchell, J. C., & Nissenbaum, H. (2006). “Privacy and contextual integrity: Framework and applications”. In Security and Privacy, IEEE Symposium, May, p.15

Laufer, R. S., & Wolfe, M. (1977). "Privacy as a concept and a social issue: A multidimensional developmental theory." Journal of Social Issues 33.3, p. 22-42

Nguyen, C.M.H., Haynes, P., Maguire, S. & Friedberg, J. (2013) A User-centred approach to the data dilemma: context, architecture and policy, in M. Hilderandt et al (Eds) Digital Enlightenment Yearbook, p.227-242

Palen, L. & Dourish, P. (2003). "Unpacking privacy for a networked world."Proceedings of the SIGCHI conference on Human factors in computing systems. ACM.

GLOSSARY OF TERMS

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

HAT-ready Device
A device that is able to send and/or receive data to/from the HAT in a way that is compliant to *HAT CoP* and certified by the *HAT project*

HAT-ready Service
A service that is able to send and/or receive data to/from the HAT in a way that is compliant to *HAT CoP* and certified by the *HAT project*

HAT Service
A service that runs on the HAT at all levels (platform, user, middleware etc.)

HAT User
An individual who owns and uses HAT data and integrates data from HAT-ready devices and services

HAT Data
Data from HAT-ready devices and services which the individual has access to that is acquired into the user's own HAT

HAT Event Data
A set of HAT data that is brought together by the HAT user for a user-defined 'event'. HAT event data could be tracked by the user over time or shared, sold, rented, traded through the D3 system

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 Developers
Individuals who create HAT services who could be working for HAT service providers

HAT Service Providers
Organisations who provide a HAT service on the HATPDP

HAT Participants HAT developers, HPPs, HAT users, HAT service providers

HAT CoP A set of practices that all HAT participants subscribe to

The D3 System The Direct Data Debit (D3) system on the HAT that enables the access of personal data on an individual's HAT

HAT Project/Foundation The £1.2m RCUK Digital Economy-funded project of 6 universities led by WMG, University of Warwick that would evolve into an open-sourced, community supported foundation

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
6. Users lookup and check personal data on their HAT
7. User create an event and decide what HAT data is relevant in the event
8. User track their HAT event data
9. User export their HAT event 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 Project/Foundation

Description: The £1.2m RCUK Digital Economy-funded project of 6 universities led by WMG, University of Warwick that would evolve into an open-sourced, community supported foundation

Functions:

1. Appoints and licenses the HATPDP hosting by HPPs
2. Supports HPPs with technical, economic and business advice
3. Advises on how devices and services can be HAT-ready
4. Reviews requests for HAT certification of HAT-ready devices and services
5. Certifies if devices and services are HAT-ready
6. Enables the download of HATPDP and its versions for HAT users by HATPDP providers
7. Maintains and updates the HATPDP
8. Maintains and updates HAT inbound APIs of all HATPDPs
9. Maintains and updates HAT outbound APIs of all HATPDPs
10. Maintains and updates HAT store catalogue of all HAT-ready devices and services

11. Manages the Framework of Accreditation on HAT service providers
12. Manages the HAT unique ID database of HAT users

13. Advises on economic and business models of the HAT
14. Regulates financial and economic conditions within the HAT ecosystem
15. Approve pricing structures of HAT applications and charge policies of HATPDP providers

HAT Developer

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 HATPDP provider 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 the HARRIET team)

The Investigators

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)

The Researchers

Funded Researchers

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

Nancy Olson WMG, University of Warwick

Charith Perera The Australian National University

Mark Skilton University of Warwick

Industry Advisory Board

Accenture
ARUP
Bosch
Cogent Elliot
DCS Europe
Dropletpay
Dyson
Enable Software
Fibaro
GlaxoSmithKline
HWP Consulting
Mydex
Osram
Sprue Aegis plc
Strand Hardware

IAB Independent Chair: Paul Tasker

http://hubofallthings.org

Acknowledgements

We gratefully acknowledge the support of the RCUK Digital Economy Theme for providing the £1.2m funding for the HAT, a research project involving six universities: Cambridge, Edinburgh, Exeter, Nottingham, Warwick, and West of England.