

Operational Framework: Institutional Controls

Daniel "Dazza" Greenwood^{1,*}, Arek Stopczynski^{1,2}, Brian Sweatt¹, Thomas Hardjono¹, Alex Sandy Pentland¹

1 MIT

2 DTU

*** E-mail: dazza@civics.com**

Contents

1	Introduction and Overview (Arek)	2
2	The New Realities of Living in a Big Data Society (Arek)	2
3	The New Deal on Data (Arek)	4
4	Personal Data: Emergence of a New Asset Class (Thomas)	6
5	Enforcing the New Deal on Data (Dazza)	9
6	Essential Elements of the New Deal of Data (Brian)	12
7	Transitioning End-User Assent Practices (Arek)	16
8	Business, Legal and Technical Dimensions of Big Data Systems (Dazza)	18
9	Big Data and Personal Data Institutional Controls (Thomas)	19
10	Scenarios of Use in Context (Dazza)	23
10.1	Example Scenario: Research Systems	24
10.2	Scenarios of Use Today, Tomorrow and the Day After	27
11	Future Research (Brian)	28
11.1	Research on Design and Deployment of Big Data Systems	29

22	11.2 Research on Big Data for Design of Institutions	31
----	--	----

23 **1 Introduction and Overview (Arek)**

24 To realize the promise and prospects of a Big Data society and avoid its security and confiden-
 25 tiality perils, institutions are updating operational frameworks governing business, legal, and
 26 technical dimensions of their internal organization and interactions with the outside world. This
 27 chapter describes how the common good can be served by framing these types of institutional
 28 rules and processes to ensure a greater user control over personal data, as well as large scale risk
 29 management and interoperability for data sharing between and among institutions.

30 The control points traditionally relied upon as part of corporate governance, management
 31 oversight, legal compliance, and enterprise architecture must evolve and expand to match op-
 32 erational frameworks for Big Data. An operational framework used for a Big Data-driven or-
 33 ganization requires a balanced set of institutional controls. These institutional controls must
 34 support and reflect greater user control over personal data and large scale interoperability for
 35 data sharing between and among institutions. Core capabilities of these controls include re-
 36 sponsive rule-based systems governance and fine-grained authorizations for distributed rights
 37 management. In the following sections we explore the emergence of the Big Data Society, out-
 38 line the ways to support it in the institutional context, and draft the future directions of research
 39 and development.

40 **2 The New Realities of Living in a Big Data Society (Arek)**

41 Sustaining a healthy, safe, and efficient society is a scientific and engineering challenge going
 42 back to the 1800s, when the Industrial Revolution spurred rapid urban growth, creating huge
 43 social and environmental problems. The remedy then was to build centralized networks that
 44 delivered clean water and safe food, enabled commerce, removed waste, provided energy, fa-
 45 cilitated transportation, and offered access to centralized healthcare, police, and educational

46 services. Those networks formed a backbone of the society as we know it today.

47 These century-old solutions are however becoming increasingly obsolete and inefficient. We
48 have cities jammed with traffic, world-wide outbreaks of disease that are seemingly unstoppable,
49 and political institutions that are deadlocked and unable to act. We face the challenges of
50 global warming, uncertain energy, water, and food supplies, and a rising population, driving
51 urbanization that will require paving 5 billion square meters of road by 2025 in China alone [1].

52 It does not have to be this way. We can have cities that are protected from pandemics, energy
53 efficient, have secure food and water supplies, and have much better government. To reach these
54 goals, however, we need to radically rethink our approach. Rather than static fixed systems,
55 separated by function — water, food, waste, transport, education, energy — we must consider
56 them as dynamic, data-driven networks. Instead of focusing only on access and distribution,
57 we need the networked and self-regulating systems, driven by the needs and preferences of the
58 citizens. We also need to create the channels for the society to agree upon and communicate
59 those needs.

60 To ensure a sustainable future society, we must use our new technologies to create a *nervous*
61 *system* maintaining the stability of government, energy, and public health systems around the
62 globe. Our digital feedback technologies are today capable of creating a level of dynamic re-
63 sponsiveness that our larger, more complicated modern society requires. We must reinvent the
64 systems of the societies within a control framework: sensing the situation, combining these obser-
65 vations with models of demand and dynamic reaction, and finally using the resulting predictions
66 to tune the system to match the demands.

67 The engine driving this new nervous system is Big Data: the newly ubiquitous digital data,
68 now available about all aspects of human life. We can analyze patterns of human experience and
69 ideas exchange within the *digital breadcrumbs* that we all leave behind as we move through the
70 world: call records, credit card transactions, GPS location fixes, among others. By recording our
71 choices, these data tell the story of our lives. This may be very different from what we decide
72 to put on Facebook or Twitter; our postings there are what we choose to tell people, edited

73 according to the standards of the day. Who we really are is even more accurately determined
 74 by where we spend our time and which things we buy, rather than just what we say we do.

75 The process of analyzing the patterns within these digital breadcrumbs is called reality
 76 mining [2,3], and through it we can learn an enormous amount about who we are. The Human
 77 Dynamics research group at MIT have found that we can use them to tell if we are likely to
 78 get diabetes [4], or whether we are the sort of person who will pay back loans [5]. By analyzing
 79 these patterns across many people, we are discovering that we can begin to explain many things
 80 — crashes, revolutions, bubbles — that previously appeared to be random acts of God [6]. For
 81 this reason the magazine Technology Review named our development of reality mining as one
 82 of the ten technologies that will change the world [7].

83 3 The New Deal on Data (Arek)

84 The digital breadcrumbs we leave behind provide clues about who we are and what we want. This
 85 makes these personal data immensely valuable, both for public good and for private companies.
 86 As European Consumer Commissioner, Meglena Kuneva said recently, “Personal data is the
 87 new oil of the Internet and the new currency of the digital world” [8]. This new ability to see
 88 the details of every interaction can be however used for good or for ill. Therefore, maintaining
 89 protection of personal privacy and freedom is critical to our future success as a society. On one
 90 hand, we need to enable even more data sharing for the public good; on the other, we need to
 91 do a much better job in protecting the privacy of the individuals.

92 A successful data-driven society must be able to guarantee that our data will not be abused;
 93 perhaps especially that government will not abuse the power conferred by access to such fine-
 94 grain data. To achieve the positive possibilities of the new society, we require the *New Deal on*
 95 *Data*, workable guarantees that the data needed for public good are readily available while at the
 96 same time protecting the citizenry [3]. We must develop much more powerful and sophisticated
 97 tools to use personal data to both build a better society and to protect the rights of the citizens.

98 The key insight that motivates the creation of the New Deal on Data is that our data are

99 worth more when shared, because these aggregated data inform improvements in systems such
100 as public health, transportation, and government. For instance, we have demonstrated that
101 data about the way we behave and where we go can be used to minimize the spread of infectious
102 disease [4, 9]. Our research has reported how we were able to use these digital breadcrumbs to
103 track the spread of influenza from person to person on an individual level. And if we can see it,
104 we can stop it. Here the result of sharing our personal data is that we can build a world where
105 the threat of infectious pandemics is greatly diminished.

106 Similarly, if we are worried about global warming, these shared, aggregated data can show
107 us how patterns of mobility relate to productivity [10]. In turn, this provides us with the ability
108 to design cities that are more productive and, at the same time, more energy efficient. But in
109 order to be able to obtain these results and make a greener world, we need to be able to see
110 the people moving around; this depends on many people willing to contribute their data, even
111 if only anonymously and in aggregate.

112 While concrete examples such as better health systems and more energy efficient transporta-
113 tion systems motivate the New Deal on Data, there is an even greater public good that can be
114 achieved by efficient and safe data sharing. To enable sharing of personal data and experiences,
115 we need secure technology and regulation that allow individuals to safely and conveniently share
116 personal information with each other, with corporations, and with government. Consequently,
117 the heart of the New Deal on Data must be to provide both regulatory standards and financial
118 incentives that entice owners to share data, while at the same time serving the interests of both
119 individuals and society at large. We must promote greater idea flow among individuals, not just
120 corporations or government departments.

121 Unfortunately, today most personal data are siloed off in private companies and therefore
122 largely unavailable. Private organizations collect the vast majority of the personal data in
123 the form of mobility patterns, financial transactions, phone and Internet communications, etc.
124 These data must not remain the exclusive domain of private companies, because then they are
125 less likely to contribute to the common good. These private organizations must be thus the key

126 players in the New Deal on Data framework for privacy and data control. Likewise, these data
 127 should not become the exclusive domain of the government, as this will not serve the public
 128 interest of transparency; we should be suspicious of trusting the government with such power.
 129 Ultimately, the entities who should be empowered to share and make decisions about their data,
 130 are people themselves: users, participants, citizens.

131 The ultimate goal is to provide the society tools to analyze and understand what needs
 132 to be done, and to reach the consensus how to do it. This goes beyond the creation of more
 133 communication platforms. The assumption that more interactions between users will result in
 134 better decisions being made, may be very misleading. Although in the recent years we have
 135 seen some great examples of using social networks for better organization in society, for example
 136 during political protests [11,12], we are not even close to the point where we can start reaching
 137 consensus about the big problems: epidemics, climate change, pollution. The discussions must
 138 be data driven, involving both experts and wisdom of the crowds. The problems we are dealing
 139 with as a now global society are not easy. We are responsible for many of them, and being able
 140 to tackle them on a global scale is necessary for our, mankind, survival.

141 4 Personal Data: Emergence of a New Asset Class (Thomas)

142 It has long been recognized that the first step to promoting liquidity in land and commodity
 143 markets is to guarantee ownership rights so that people can safely buy and sell. Similarly, the
 144 first step toward creating greater idea and idea flow (‘idea liquidity’) is to define ownership rights.
 145 The only politically viable course is to give individual citizens rights over data that are about
 146 them and in fact, in the European Union these rights flow directly from the constitution. We
 147 need to recognize personal data as a valuable asset of the individual that is given to companies
 148 and government in return for services.

149 The simplest approach to defining what it means to own your own data is to draw an analogy
 150 with the English common law ownership rights of possession, use, and disposal:

- 151 • You have the right to possess data about you. Regardless of what entity collects the data,
152 the data belong to you, and you can access your data at any time. Data collectors thus
153 play a role akin to a bank, managing the data on behalf of their customers.
- 154 • You have the right to full control over the use of your data. The terms of use must be opt-
155 in and clearly explained in plain language. If you are not happy with the way a company
156 uses your data, you can remove the data, just as you would close your account with a bank
157 that is not providing satisfactory service.
- 158 • You have the right to dispose of or distribute your data. You have the option to have data
159 about you destroyed or redeployed elsewhere.

160 Individual rights to personal data must be balanced with the need of corporations and govern-
161 ments to use certain data-account activity, billing information, and so on-to run their day-to-day
162 operations. This New Deal on Data therefore gives individuals the right to possess, control, and
163 dispose of copies of these required operational data, along with copies of the incidental data
164 collected about you such as location and similar context.

165 Note that these ownership rights are not exactly the same as literal ownership under modern
166 law, but the practical effect is that disputes are resolved in a different, simpler manner than
167 would be the case for (as an example) land ownership disputes.

168 In 2007, one author (Pentland) first proposed the New Deal on Data to the World Economic
169 Forum [13]. Since then, this idea has run through various discussions and eventually helped
170 shape the 2012 Consumer Data Bill of Rights in the United States, along with a matching
171 declaration on Personal Data Rights in the EU. These new regulations hope to accomplish the
172 combined trick of breaking data out of the current silos, thus enabling public goods, while at
173 the same time giving individuals greater control over data about them. But, of course this is
174 still a work in progress and the battle for individual control of personal data rages onward.

175 The World Economic Forum (WEF) has dubbed personal data as the “New Oil” or resource
176 of the 21st century [13]. The discovery of oil and the subsequent development of the oil industry

over the past 100 years has spurred not only the development of the automobile industry but also the creation of the global transportation infrastructure, including the massive freeway networks that we see today in the developed nations. The “personal data sector” of the economy today is still in its infancy, its state akin to the oil industry at the late 1890s prior to the development of the Model-T Ford automobile. The productive collaboration between the Government (building the state owned freeways), the private sector (mining and refining oil, building automobiles) and the citizen (the user-base of these services) allowed the develop nations to expand its economies by creating new markets adjacent to the automobile and oil industries.

If personal data as the new oil is to reach its global economic potential, there needs to be a productive collaboration between all the stakeholders in the establishment of a *personal data ecosystem*. As mentioned in [13] a number of fundamental questions about privacy, property, global governance, human rights - essentially around who should benefit from the products and services built upon personal data - are major uncertainties shaping the opportunity. The rapid rate of technological change and commercialization in using personal data is undermining end user confidence and trust.

The current personal data ecosystem is fragmented and inefficient. Too much leverage is currently being accorded to service providers that on-board and register end-users. These siloed repositories of personal data exemplifies the fragmentation of the ecosystem. These repositories contain data of varying qualities. Some are attributes of persons that are unverified, while other represent higher quality data that have been cross-correlated with other data points of the end-user.

For many participants, the risks and liabilities exceed the economic returns. Besides not having the infrastrcuture and tools to manage personal data, many end-users simply do not see the benefit of fully participating in the ecosystem. The current focus of many Internet-based service providers is to capture as much personal data from the end-user and to sell this data into the advertising industry. Personal privacy concerns are thus inadequately addressed at best, or simply overlook in the majority of the cases. The current technologies and laws fall short

204 of providing the legal and technical infrastructure needed to support a well-functioning digital
 205 economy.

206 The report of the World Economic Forum [13] also suggest a way forward by recommending
 207 a number of areas where efforts could be directed:

- 208 • Alignment of key stakeholders: Citizens, the private sector and the public sector need to
 209 work in support of one another. Efforts such as NSTIC [?] – albeit still in its infancy –
 210 represents a promising direction for a global collaboration.
- 211 • Viewing “data as money”: There needs to be a new change in mindset where an individual’s
 212 personal data items are viewed and treated in the same way as their money. These personal
 213 data items would reside in an “account” (like a bank account) where it would be controlled,
 214 managed, exchanged and accounted for just like personal banking services operate today.
- 215 • End-user centricity: All entities in the ecosystem need to recognize that end-users are
 216 vital and independent stakeholders in the co-creation and value exchange of services and
 217 experiences. Efforts such as the *User managed Access* (UMA) initiative [?] point in the
 218 right direction by designing systems that are user-centric and managed by the user.

219 5 Enforcing the New Deal on Data (Dazza)

220 How can we enforce this New Deal? The threat of legal action alone is important, but insufficient,
 221 because if you cannot see abuses then you cannot prosecute them. Moreover, who wants more
 222 lawsuits anyway? Enforcement can be addressed in significant ways without prosecution of
 223 public statute or regulation at all. In many fields, companies and governments rely upon multi-
 224 party frameworks of agreed rules governing common business, legal and technical practices to
 225 create effective self-organization and enforcement. These approaches hold promise as a method
 226 for using institutional controls to form a reliable operational framework balancing the needs for
 227 big data, privacy and access.

228 One current best practice is a system of data sharing called trust networks. Trust networks
229 are a combination of networked computers and legal rules defining and governing expectations
230 regarding data. With respect to data belonging to individuals, these networks of technical and
231 legal rules keeps track of user permissions for each piece of personal data, and a legal contract
232 that specifies both what you can and cannot do with the data and what happens if there is a
233 violation of the permissions. For example, in such a system all personal data can have attached
234 labels specifying what the data can, and cannot, be used for. These labels are exactly matched
235 by the network's system rules and terms in legal contracts between all the participants stating
236 penalties for not obeying the permission labels. These rules can, and often do, reference or
237 require audits of relevant systems and data use, demonstrating how traditional internal controls
238 can be leveraged as part of the transition to more novel trust models.

239 Complete tracking and regulation of every aspect of a trust network is not the goal or
240 even desirable in order to achieve effective enforcement. Rather, the rules for a trust network
241 align enforcement with the highest priority issues and those upon which trust of participants is
242 premised. The relevant issues arise from the dynamics of data flows, underlying trust models
243 and contextual scenarios within which the networked data and the relationships of parties in the
244 trust network. When a trust network involves use of personal data, then the user permissions and
245 corresponding limits on use are fundamental to the trust model. In this context, the permissions,
246 including the provenance of the data, should require appropriate levels of audit. A well designed
247 trust network, elegantly integrating computer and legal rules, allows automatic auditing of data
248 use and allows individuals to change their permissions and withdraw data.

249 Having system rules applicable to the networks, applications and data as well as all the ser-
250 vices providers other intermediaries, and the users themselves is the mechanism for establishing
251 and operating a trust network. System rules are sometimes called operating regulations in the
252 credit card context, or known as trust frameworks in the identity federations context, or trading
253 partner agreements in a supply value chain context. There are many general examples of multi-
254 party shared architectural and contractual rules that share the generic characteristic of creating

binding obligations and enforceable expectations on all participants in scalable networks. Another common characteristic of the system rules design pattern is that the participants in the network can be widely distributed across very heterogeneous business ownership boundaries, legal governance structures and technical security domains. Yet, the parties need not agree to conform all or most aspects of their basic roles, relationships and activities in order to connect to to systems of a trust network. Cross-domain trusted systems must, by their nature, focus mandatory and enforceable rules narrowly upon the critical items that must be commonly agreed in order for that network to achieve it's purpose.

For example, institutions participating in credit card and automated clearinghouse debit transactional networks are subject to profoundly different sets of regulations, business practices, economic conditions and social expectations. The network rules focus upon the topmost agreed items affecting interoperability, reciprocity, risk and revenue allocation. The knowledge that fundamental rules are subject to enforcement actions is one of the foundations of trust as well as a motivation to prevent or address violations before they trigger penalties. A clear example of this approach can be found with the Visa Operating Rules, covering a vast global real-time network of parties that agree to rules governing their roles in the system as merchants, banks, transaction processors, individual or business card holders and other key system roles.

A system like this has made the interbank money transfer system among the safest systems in the world and the daily backbone for exchanges of trillions of dollars, but until recently such systems were only for the 'big guys. To give individuals a similarly safe method of managing personal data, the Human Dynamics research group here at MIT, in partnership with the Institute for Data Driven Design, co-founded by John Clippinger and one author (Pentland), have helped build openPDS (open Personal Data Store) <http://openPDS.media.mit.edu> for project information and <https://github.com/HumanDynamics/openPDS> for the open source code.

The openPDS system is a consumer version of a personal cloud trust network and we are now testing it with a variety of industry and government partners. Soon, sharing your personal data could become as safe and secure as transferring money between banks.

282 The Human Dynamics Lab has applied the system rules approach to development of inte-
 283 grated business, technical architecture and rules large scale institutional use of personal data
 284 stores, available as an example under MIT’s creative commons license by MIT, at: github.com/HumanDynamics/

285 The capacity to apply the appropriate methods of enforcement for a trust network depend
 286 upon a clear understanding and agreement among parties about the purpose of the trusted
 287 system and the respective roles or expectations of those connecting is as participants. Therefor,
 288 an anchor is needed to a clear context of a big data operational framework and institutional
 289 controls appropriate for access and confidentiality or privacy. The following section posits the
 290 trust model and signature traits of such a context, through the lens of the New Deal on Data.of
 291 those connecting is as participants. Therefor, an anchor is needed to a clear context of a big
 292 data operational framework and institutional controls appropriate for access and confidentiality
 293 or privacy. The following section posits the trust model and signature traits of such a context,
 294 through the lens of the New Deal on Data.

295 **6 Essential Elements of the New Deal of Data (Brian)**

296 The New Deal on Data restates the controls and expectations people have with respect to their
 297 private property and personal affects and applies it to their personal data and online affects.
 298 Institutional controls must align with the New Deal on Data by providing responsive, rule-based
 299 systems governance and fine grained authorizations for distributed rights management.

300 Our lives are embedded within institutions. We are citizens of countries and cities, receive
 301 services from telecom operators, and search for things to buy in online stores. Almost any action
 302 we perform generates data, and those recordings of our lives are an important part of the Big
 303 Data promise. The data are not curated by us, but are collected ‘as is’ - and reflect our lives.

304 Today, all of the data people generate are stored in closed silos belonging to institutions
 305 providing customer services. Phone providers own mobility traces for their users, while music
 306 services store and use data on musical preferences.

307 For these data to be useful to society, the silos must be opened, and the data must be

integrated across institutions far more than they are today. If access to data for the purpose of creating value—either for the user or the society—is very limited, it does not matter how big the data is. The value of the data lies not just in the fact that they exist, but rather the knowledge, understanding, and wisdom we gain from them. It is an even bigger challenge to open up the data from disparate silos. Accessing multi-faceted data, which exist under multiple jurisdictions, about people may be prohibitively difficult. Silos are hard to crack open. Despite these difficulties, such data, not just big, but deep, covering multiple facets of a person’s life, may be invaluable for research.

Recently, we have shown how challenging, but also feasible, it is to open such institutional Big Data. In the Data For Development (D4D) Challenge ¹, the telecom operator Orange opened access to a large dataset of call detail records (CDRs) from the Ivory Coast. Working with the data as part of a challenge, teams of researchers came up with life-changing insights for the country. For example, one team developed a model for how disease spread in the country and demonstrated that information campaigns based on one-to-one phone conversations among members of social groups can be an effective countermeasure [14]. In releasing and analysing this data, the privacy of the people who generated the data was protected not only by the technical means, such as removal of the Personally Identifiable Information (PIIs), but also by legal means, with the researchers signing an agreement they will not use the data for re-identification or other nefarious means. As we have seen in several cases, such as the Netflix Prize privacy disaster [15] and other similar privacy breaches [16], true anonymization is extremely hard. Some of the weight of privacy protection must rest on the legal framework.

Opening data from the silos by publishing static datasets is important, but it is only the first step. We can do even more substantial things when the data is available in real time and can become part of a society’s nervous system. Epidemics can be monitored and prevented in real time [4], underperforming students can be helped, and people with health risks can be treated before they get sick [17]. The same data can potentially be used for stalking, burglarizing one’s

¹<http://www.d4d.orange.com/home>

home, and as justification to charge people more for an insurance policy.

In the Unique in the Crowd project [18], de Montjoye et al. showed that even though human beings are highly predictable [19], we are also very unique. Having access to one dataset, it is easy to uniquely fingerprint someone based on just few datapoints, and use this fingerprint to discover their true identity. The higher the resolution of the data, the easier it gets to identify a person from this type of data.

The question of privacy in this context effectively becomes a question of control:

Who can release the data of one's movements? To whom? How much and how often? The data are collected by the institution. The data are about people who not even be aware that they exist, and certainly do not own them. People cannot decide upon them, cannot review them. People cannot delete them. Very few parties can use the data, even if people wanted them to. For systems to be truly data driven and capable of transitioning to the networked and highly dynamic assumptions of a big data economy, the key agreements reflected in trust networks must reflect a new deal. The operating frameworks of successful institutions are capable of balancing interests in access, confidentiality and every day reliance upon big data including personal and other sensitive information. The institutional controls relevant to achieve, maintain and appropriately adapt these balances support and reflect adherence to the fair information practices.

[Footnote: HEW Report, OECD rendition, EU Directive, DHS/NSTIC version, MGL FIPA and culminating in New Deal on Data adaptation].

Within the existing legal frameworks, it is possible to change the vantage point of the data ownership and put the user, the entity about whom the data are, in control. This may be achieved by providing a copy of the data to a personal silo, which is provided by or on behalf of the user. The user would become the owner of their copy of the data, or whenever possible the original, in the old Common Law sense with the right to use, transfer, and delete the data. An example of such a mechanism in an institutional context is the Blue Button initiative ², where

²<http://www.healthit.gov/bluebutton>

360 the patients can get a copy of their health records. Once the copy is with the user, they can do
361 with it as they wish: give it to someone, make it public, do research on it, destroy it.

362 Under such a system, users can accumulate data about themselves from multiple sources.
363 Information on healthcare records, mobility patterns, favorite movies, etc., all belong to the user
364 and can be accessed based on their authorization. This changes how and what data that can
365 be obtained for the purpose of research and providing services. Rather than gaining access to
366 the movements of millions of people from a telecom operator, one can potentially gain access
367 to a smaller number of much richer datasets describing the users from the mobility, health, and
368 shopping perspectives. New startups would not have to build the user profile from scratch, but
369 can offer competitive services based on the user's previously-collected data from day one. Users
370 can immediately get better services, using their data in new places.

371 The first, operational challenge of moving towards end-user data ownership on a large scale,
372 is to create an ecosystem where such user-owned data are known and accessible. We are currently
373 embedded in a feudal framework: Facebook owns the data generated by and about their users,
374 and provides access to this data to 3rd parties that the user might or might have not directly
375 authorized. It is reasonably easy for users to download all their data from these services, such as
376 Facebook. It is reasonably easy to put it on a public file-sharing site, such as a user's personal
377 Dropbox, or even create a myself-API, becoming a self-hosted API to one's own personal data.
378 The challenge is to have clients talk to this API and provide services, rather than going to
379 Facebook for one's data. Today, virtually no online service is configured to access user data
380 directly from the user. This is at least partly due to their not being an open, widely implemented
381 standard for providing self-hosted data services for users. We have done slightly better on the
382 Internet scale with identity: one can deploy their own OpenID server fairly easily, and many
383 services will allow the user to sign in. We should be heading in the same direction with data.

384 7 Transitioning End-User Assent Practices (Arek)

385 The way the user grants authorizations to the data she owns is not a trivial matter. The flow of
 386 personal information, such as location data, purchases, health records, etc. can be very complex.
 387 Every tweet, every geo-tagged picture, every phone call, and every purchase with credit card,
 388 provide the user's location not only to the primary service, but also to all the applications and
 389 services that have been authorized to access and re-use these data. The authorizations may
 390 come from the end-user or, often, be granted by the collecting service, based on an umbrella
 391 terms of service, allowing the re-use of the data. Implementation of such flows was a crucial
 392 part of the Web 2.0 revolution, realized with RESTful APIs, mashups, and authorization-based
 393 access. The way the data travel between the services has however become arguably too complex
 394 for a user to handle and manage.

395 Increasing the amount of data the user controls and granularity of this control is meaningless
 396 if it cannot be exercised in an informed way. For many years, the End User License Agreements
 397 (EULAs), long incomprehensible texts have been accepted blindly by the end-user, trusting they
 398 have not agreed to anything that could harm them. The process of granting the authorizations
 399 cannot be too complex, as it would prevent the user from understanding her decisions. At
 400 the same time, it cannot be too simplistic, as it may not sufficiently convey the weight of the
 401 privacy-related decisions. It is a challenge in itself, to build the end-user assent systems that
 402 allow the user to understand and adjust their privacy settings. Complex EULAs do not promote
 403 the privacy of the users, effectively pushing them to press *I Agree* in every presented window.
 404 The consequences of those assent actions are not emphasized; as the data being collected is
 405 becoming increasingly complex and our computations more sophisticated, every act of sharing
 406 can lead to great benefits to the society, but also make the users vulnerable.

407 This gap between the interface, the single click, and the effect, can render the data owner-
 408 ship meaningless; the click may wrench people and their data into systems and rules that are
 409 antithetical to fair information practices, such as is prevalent with today's end-user licenses in
 410 cloud services or applications. Managing the potentially long term and opposite dynamics fueled

411 by old deal systems operating simultaneously with the new deal systems is an important design
412 and migration challenge during the transition to a Big Data economy. During this transition
413 and after the New Deal on Data is no longer new, personal data must continue to flow in order
414 to be useful. Protecting the data of people outside of the user-controlled domain is very hard
415 without a combination of cost effective and useful business practices, legal rules, and technical
416 solutions. For these reasons, the Human Dynamics group has focused upon and collaborated
417 with partners to support the clarification of business, legal, and technical short- and longer-term
418 viable solutions.

419 We envision Living Informed Consent, where the user is entitled to know what data is being
420 collected about her by which entities, empowered to understand the implications of data sharing,
421 and finally put in charge of the sharing authorizations. We suggest the readers ask themselves a
422 question: *Which services know which city I am in today?*. Google? Apple? Twitter? Facebook?
423 Flickr? This small application we have authorized a few years ago to access our Facebook
424 check-ins and forgot since then? This is an example of a fundamental question related to user
425 privacy and assent, and yet finding the answer to it may be surprisingly difficult in today's
426 ecosystem. We can hope that most of the services treat the data responsibly and according to
427 user authorizations. In the complex network of data flows however, it is relatively easy for the
428 data to leak to services careless with it or simply malicious [20].

429 It is clear that the promise of the Big Data can only be realized when the data is shared,
430 available even more than it is today. For this, the user herself should be put in the driver's
431 seat and made decisions about who is authorized to see what and for what purpose. To realize
432 this, the solutions for making the user decisions well thought-through must be designed and
433 implemented.

434 8 Business, Legal and Technical Dimensions of Big Data Sys- 435 tems (Dazza)

436 When it comes to data intended to be accessible over networks-whether big, personal or otherwise-
437 the traditional container of an institution makes less and less sense. Institutional controls apply,
438 by definition by or to some type of institutional entity such as a business, governmental or reli-
439 gious organization. A combined view of the business, legal and technical facts and circumstances
440 surrounding big data is necessary to know what access, confidentiality and other expectations
441 exist. The relevant contextual aspects of big data of one institutional is often profoundly dif-
442 ferent from that of another. As more and more organizations use and rely upon big data, a
443 single formula for institutional controls will not work for increasingly heterogeneous business,
444 legal and technical environments in play.

445 Looking at an institution as a business, legal and technical system is one effective approach
446 for dealing with the inherent complexity of managing heterogeneous and distributed networks
447 of actors and interactions. The business models, interface-point operational practices and rel-
448 evant assumptions must be consistent and frequently carefully agreed at an executive level by
449 and with institutions as part of the value exchange involving data and access to high value,
450 mission critical or sensitive systems and services. The applicable legal frameworks, common
451 assumptions regarding likely allocation of liability and resolution of disputes in the event of
452 losses and expected types of contracting practices need to reflect and support the business goals
453 and purposes for the system and data. When technical standards are selected, configured and
454 applied to systems they too must support and reflect the business and legal dimensions and be
455 supported and reflected by those dimensions.

456 Once a systems view is adopted, there is a tractable starting point to narrow or broaden
457 the scope of view to see the smaller and larger systems and to make better and more effective
458 use and control of big data. Within a given institution, there may in fact be many different
459 discernable institutions and corresponding systems and any given system of one institution will

frequently in fact exist across many different discernable institutions. However, defining as a system the thing to which institutional controls apply provides an achievable and measurable basis for balancing privacy, access and other interests in big data.

Many organizations are structured with clear leadership on business, legal and technical issues functionally assigned to top level executive roles. Business issues are typically allocated to roles such as CEO, COO or CFO, while leadership on legal issues is commonly assigned to roles like general counsel and regulatory compliance and technical leads are often the roles of CIO, CTO or CSO. Having top level leadership for each of the business, legal and technical aspects of a trust network is a critical success factor.

9 Big Data and Personal Data Institutional Controls (Thomas)

The phrase "institutional controls" refers to safeguards and protections by use of legal, policy, governance and other non-strictly technical, engineering or mechanical measures. The phrase institutional controls in a big data context can perhaps best be understood by examining how the concept has been applied to other domains. The most prevalent use of institutional controls, per se, has been in the field of environmental regulatory frameworks.

A good example of how this concept supports and reflects the goals and objectives of environmental regulation can be found in the policy documents of the EPA. This following definition is instructive, and is part of the Institutional Control Glossary of Terms [21]:

"Institutional Controls - Non-engineering measures intended to affect human activities in such a way as to prevent or reduce exposure to hazardous substances. They are almost always used in conjunction with, or as a supplement to, other measures such as waste treatment or containment. There are four categories of institutional controls: governmental controls; proprietary controls; enforcement tools; and informational devices."

Going deeper, the article by DeMeo and Doar [22] defines institutional controls thusly:

485 ”Institutional controls are administrative and legal controls that help minimize the
486 potential for human exposure to contamination and/or protect the integrity of the
487 physical remedy. They can include recorded restrictive covenants, but land use
488 laws and regulations, deed restrictions, department consent orders, and conservation
489 easements are all institutional controls.”

490 In domains of information technology, this approach is most commonly reflected as “enter-
491 prise controls” related to security. See, for example, the report [23] stating: ”Enterprise mobility
492 technologies, especially those designed to retrofit enterprise controls on top of consumer mobile
493 devices, are rapidly evolving. This was a message we heard loud and clear in the study.” This
494 study and analysis also reveals much about the internal controls needed to accommodate mobile
495 device use by employees. In both capacities as employee, consumer and other roles, the use of
496 mobile devices triggers myriad legal, policy and other implications for institutional controls.

497 In the legal domain, this concept frequently emerges under the moniker “regulatory compli-
498 ance” or “legal compliance” anchored in legal and regulatory frameworks such as HIPAA and
499 Sarbanes-Oxley (SOX). These statutory legal frameworks require covered organizations to es-
500 tablished integrated sets of governance, legal, transactional, security and other internal controls
501 to avoid violating the rules. The institutional controls are accomplished in tight integration with
502 engineering and other measures in order to ensure compliance and to control legal and security
503 risk. The use of institutional controls of this type are fundamental methods for achieving and
504 maintaining the transition to a digital, networked and big data footing for any private company,
505 government agency or other organization.

506 Consider again the analogy of institutional controls in the context of environmental law, and
507 how these types of measures can be applied in the big data, privacy and access context to digital
508 environments. Given the relatively mature and stable state of environmental regulation, there is
509 much to be learned by examining this context of institutional controls. Environmental regulatory
510 compliance with waste management cleanup requirements could include institutional controls
511 restricting land use on adjacent property. In these situations, it is possible that the remediation

strategy requires significant use of land outside the property boundaries of the cleanup site. In these cases, the regulators and the land owner responsible for the regulated property must find ways to ensure a common approach among multiple owners and across multiple property environments. Use of measures such as a clauses on the relevant deeds, an enforceable consent order or regulations and zoning rules are examples of more severe institutional controls that can be employed to ensure consistent and effective actions are taken across ownership and real property boundaries.

See, for example, FDEP, Division of Waste Management [24] which states that “...RMO III does contemplate contamination beyond the Property boundaries, which would require agreement by the adjacent owners to put an RC on their properties as well.”

The concept of an “institutional control boundary” is especially clarifying and powerful when applied to the networked and digital boundaries of an institution. In the context of Florida’s environmental regulation frameworks, the phrase is applied to describe the various types of combinations risk management levels related to target cleanup standards and extend beyond the area of a physical property boundary. See the Final Technical Report: Development of Cleanup Target Levels (CTLs) for Ch. 62-777, F.A.C. [25] stating “Risk Management Options Level III, like Level II, allows concentrations above the default groundwater CTLs to remain on site. However, in some rare situations, the institutional control boundary at which default CTLs must be met can extend beyond the site property boundary.”

The EPA provides considerable information on the nature and use of institutional controls, including situations when the situational scope extends to adjacent properties owned by third parties. See, generally, *EPA Hazardous Waste Corrective Action Guidance on Institutional Controls* citeEPA2007. Also see: *Institutional Controls Bibliography: Institutional Control, Remedy Selection, and Post-Construction Completion Guidance and Policy, December 2005* [26].

When institutional controls would apply to “separately owned neighboring properties” a number of issues arise. Engagement with affected third parties, requiring the party responsible for site cleanup to use “best efforts” to attain agreement by third parties to institute the relevant

539 institutional controls, use of third party neutrals to resolve disagreements regarding the applica-
540 tion with institutional controls or forcing an acquisition of the neighboring land by forcing the
541 party responsible to purchase the property of by purchase of the property directly by the EPA.
542 See [27].

543 In the context of big data, privacy and access, institutional controls are seldom if ever the
544 result of government regulatory frameworks such as are seen in the environmental waste man-
545 agement oversight by the EPA. Rather, institutions applying measures constituting institutional
546 controls in the big data and related information technology and enterprise architecture contexts
547 will typically employ governance safeguards, business practices, legal contracts, technical se-
548 curity, reporting and audit programs and a various risk management measures. Inevitably,
549 institutional controls for big data will have to operate effectively across institutional boundaries
550 just as environmental waste management internal controls must sometimes be applied across
551 real property boundaries and may subject multiple different owner to enforcement actions corre-
552 sponding to the applicable controls. Short of government regulation, the use of system rules as
553 a general model are one widely understood, accepted and efficient method for defining, agreeing
554 and enforcing institutional and other controls across business, legal and technical domains of
555 ownership, governance and operation.

556 The use of system rules and integrated participation agreements by developers and end-
557 users is a way to ensure intended operational frameworks conform to applicable institutional
558 controls. The example of “living consent” described below, demonstrates how institutional
559 controls comprised of legal and definite workflow measures in concert with technical methods
560 can result in a higher level of performance while appropriately balancing legitimate interests of
561 various parties regarding use and access to personal data.

562 Following the recommendation of the World Economic Forum recommendations of treating
563 personal data stores in the manner of bank accounts [13], there are a number of infrastructure
564 improvements that need to be realized if the personal data ecosystem is to flourish and deliver
565 new economic opportunities. We believe the following infrastructure improvements are necessary

566 for the coming personal data ecosystem:

- 567 • *New global data provenance network*: In order for personal data to be treated like bank
 568 accounts, the origin information regarding data items coming into the data store must be
 569 maintained. In other words, the provenance of all data items must be accounted for by
 570 the IT infrastructure upon which the personal data store operates. The heterogeneous
 571 provenance databases must then be interconnected in order to provide a resilient and
 572 scalable platform for audit and accounting systems to track and reconcile the movement
 573 of personal data from the respective data stores.

- 574 • *Trust network for computational law*: In order for trust to be established between parties
 575 who wish to exchange personal data, we foresee that some degree of “computational law”
 576 technologies may have to be integrated into the design of personal data systems. Such
 577 technologies should not only verify terms of contracts (e.g. terms of data use) against
 578 user-defined policies but also have mechanisms built-in to ensure non-repudiation of entities
 579 who have accepted these digital contracts. Efforts such as [28, 29] are beginning to bring
 580 non-repudiation and enforceability of contracts into the technical protocol flows.

- 581 • *Development of Institutional Controls for Digital Institutions*: Currently there are a number
 582 of proposal for the creation of virtual currencies (e.g. BitCoin [30], Ven [31]) in which the
 583 systems have the potential to evolve into self-governing “digital institutions“ [?]. Such
 584 systems and insitutions that operate on them will necessitate the development of a new
 585 paradigm to understand the aspects of institutional control within their context.

586 10 Scenarios of Use in Context (Dazza)

587 Supporting the effective development of institutional controls for big data requires an under-
 588 standing of how to define and work with the applicable context surrounding the scenarios within
 589 which the big data exists. In particular, the New Deal on Data will require a set of Institutional
 590 Controls involving governance, business, legal and technical aspects that are knowable only with

reference to the relevant context of a factually based scenario of use. The following scenarios demonstrate signature features of the New Deal on Data in various contexts and serve as an anchor to evaluate what Institutional Controls are well aligned.

10.1 Example Scenario: Research Systems

Computational Social Science (CSS) studies are based on data collected often with an extremely high resolution and scale. Using computational power combined with mathematical models, such data can be used to provide insights into human nature. Much of the data collected, for example mobility traces are sensitive and private; most individuals would feel uncomfortable sharing them publicly. The need for solutions to ensure the privacy of the individuals has grown alongside the data collection efforts.

The data collection in the CSS context is based on the informed consent of the participants. Countries have different bodies regulating such studies, for example Institutional Research Boards (IRBs) in the US. Although certain minimal requirements for implementing informed consent exist[TODO: reference], they are often not very well suited for the large-scale studies, where the amount and sensitivity of the data calls for sophisticated privacy controls. As the scale of the studies grows, in terms of the number of participants, collected bits per user, and duration, the EULA-style informed consent is no longer sufficient and makes it hard to claim that participants in fact expressed informed consent.

This year we have deployed a 1,000 phones study at Technical University of Denmark, where we handed out mobile phones to freshmen students in order to study their networks and social behavior in the important change moment of their lives, when they join the university. The study, called SensibleDTU, uses not only data collected from the mobile phones (location, Bluetooth-based proximity, call and sms logs etc.) but also data collected from social networks, questionnaires filled out by participants, behavior in economic games and so on. As the data is collected in the context of the university, there is potentially a big issues of students feeling obliged to participate in the study, feeling that their grades may depend on it, or that the data

617 may influence their grades. In this context, we see the implementation of Living Informed Con-
618 sent not only as a technical mean to put participants in control of the data we collect, but also
619 to convey the message about the opt-in nature of the study, the boundaries of the data usage,
620 and parties accessing the data.

621 It is not feasible to explain the terms and answer all the questions to all 1,000 students
622 personally. The controls must be self-explanatory as much as possible, and guide the user from
623 the first opening of the link to the study to the grant of the authorizations. At the same time,
624 every click made by the user, should be an expression of an informed decision, so the user journey
625 must be a balance of guidance and understanding. For this reason we have created a set of web
626 applications, allowing the users to enroll into the study, express informed consent, and interact
627 with their data.

628 As the study will last for several years, hopefully allowing us to see the life of a student from
629 the very first friendships made until the graduation party, the consent must remain alive. It is
630 again a matter of balance: we do not want the participants to feel under constant surveillance
631 (as they are not, the data is used mostly in aggregated form), at the same time to remember that
632 in fact, the data is being collected and used. We are still trying to understand how to achieve
633 this equilibrium: how often should we remind the users about the collection effort? should they
634 re-authorize applications from time to time? We see a great hope in the applications we create
635 for the users to provide certain services, simple such as life-logging where they can see how
636 active they are, what are their top places etc. and more advanced, such as artistic visualizations
637 of their social networks. Making the user aware of the data by transforming them into value,
638 can greatly benefit the privacy, making users constantly aware what is being collected, but also
639 what kind of value they can get out of it.

640 When a study of such scale is deployed, the particular experiments and sub-studies may
641 not be exactly defined from the very beginning. The initial deployment is a creation of a
642 testbed, where shorter or longer experiments can take place; for example part of the population
643 may participate in the experiment of quantifying the impact of feedback application on their

644 activity levels. Being able to create such experiments in an efficient way is a huge value for the
645 researchers. To do that in the most frictionless way, we give the users the choice to opt-in to
646 those additional experiments, providing some financial or other benefits. This is only possible
647 if there is a notion of identity of the participants, stronger and more useful than a piece of
648 paper with a signature. This identity allows us to reach out to people, offer them additional
649 experiments, and let them agree or disagree to them.

650 This touches upon the re-usability of data, as the new experiments may require additional
651 data to be collected, but also have access to all the existing data, based on user authorization.
652 We can imagine going even further, where entirely different studies can re-use participants data
653 from a previous study based on their authorization. When the data are owned by the users,
654 they are free to authorize access to them to any party that requests it. We can see a New Deal on
655 Data pattern here: rather than services (studies) talking to each other about the user data, they
656 talk directly to the users, seeking their authorization. This can address a very important problem
657 in the research context, the data re-use in a privacy-aware manner. Rather than publishing a
658 static dataset, where the users have lost control over their data, live and fresh data can be
659 continuously accessed by any study that the user agrees to be a part of.

660 Many studies will be willing to offer money or other value for the access to the data. Other
661 will provide the user the opportunity to have new data collected. This way, the data collection
662 becomes an opportunity for the user to enrich their personal dataset, and to benefit from it
663 in the future. Join our study and we will provide you with a smartphone and collect your
664 movement patterns for a year; we will do science and you will gain new data that can get you
665 better value or deals in different services. You may now be eligible for a different study. Or your
666 music recommendation may get better, because your music service can make a use of this extra
667 data. Your data.

668 10.2 Scenarios of Use Today, Tomorrow and the Day After

669 By inquiring into and noting the four facets of relevant context described above, it is possible
 670 to describe the basic material contours of any scenario within which big data exists such that
 671 the operational framework and adequate approaches to access, use, confidentiality and other key
 672 interests can be sustainably balanced. In a commercial scenario the relevant people might be a
 673 consumer, merchants, banks, products manufacturers, third party app developers and individual
 674 members of that consumers bowling team. The relevant transactions might be a purchase of
 675 goods by the consumer from the merchant and the corresponding app that was embedded in
 676 the goods and the downstream transaction of involving the consumer now transacting with the
 677 merchant bowling alley and interacting with a bowling team, with whom activity and sports
 678 performance data are shared and aggregated and further mashed up. The rest of the con-
 679 text can be described for any given scenario and this all could be expressed specifically rather
 680 than by role simply by running a report from the system to indicate it was in fact John Doe,
 681 of openpds.org/owner/571 purchasing a smart bowling ball from Bowl-a-Tronic of bowlapp-good.com/store/221 and so on for each party that played a role in the relevant scenario. The
 682 same techniques, used for scenarios in other economic sectors and social endeavors shed light
 683 on the fundamental nature and implications of big data and options for the use of operational
 684 frameworks acting across domains to balance privacy and access, among other interests.

686 This book represents a high value opportunity to take stock of the current state and domi-
 687 nant trends related to big data and help to illuminate important choices at a moment of early
 688 adoption, dynamic innovation and wide open possibilities. By contemplating the relevant con-
 689 texts of todays scenarios of use in, say, the fields of education, entertainment, government,
 690 manufacturing, transportation and many other core anchors of human activity, we have traction
 691 to postulate how todays prevailing trends are likely to result and what changes perhaps quite
 692 small but of profound long term impact could lead to materially different better outcomes.
 693 Consider that if the essence of the New Deal on Data were accepted today, or soon, the na-
 694 ture, tenor, capabilities and experience of living by future generations could be unrecognizably

695 better. Simply extrapolate from the current anomalous practices regarding personal data and
 696 individual identity and push forward the timeline by 5, 10, 20 years and beyond. The current
 697 trajectory ends up with dystopian scenarios that effectively reverse hard fought but easily lost
 698 constitutional deal of the United States and social compact of common law societies.

699 By contrast, by adopting the New Deal on Data now it is possible to set conditions that
 700 promote prosperity and invention even before the New Deal on Data frameworks are formally
 701 launched. This is because the uncertainty and confusion about the basic premises and expecta-
 702 tions around personal data and identity will be resolved and so investment and risk taking on
 703 a firm foundation can be unleashed. The value of big data can be accessed at less direct cost
 704 and lower risk when uncertainties about privacy liability are addressed and significant the new
 705 value is created by enabling wide scale permission based access to personal data and compu-
 706 tations about such data. Adopting use of personal data services in phases, such one economic
 707 sector, transaction type or data type at a time enables access to the lower costs and new value
 708 in a reasonable manner that allows for time to prepare for and stage each phase of adoption.
 709 By staging and phasing the New Deal on Data typical objections to change based on grounds
 710 of cost, disruption or over regulation can be addressed. Policy incentives can further address
 711 these objections, such as allowing safe harbor protections for conduct of organizations operating
 712 under the rules of a trust network. Policy makers can resolve other difficulties by combina-
 713 tions of strategic transition management methods like allowing safe harbor compliance delays,
 714 or approving alternative adoption paths and granting other non-substantive waivers to ease any
 715 burdens of migrating to new business methods. The key point is change management can be
 716 designed to achieve enough value at every phase for every key stakeholder group such that self
 717 interests and the broader interests are all aligned with the public good.

718 **11 Future Research (Brian)**

719 Our traditional methods of testing and improving government, organizations, and so on are of
 720 limited use in building a data driven society. Even the scientific method as we normally apply it

721 doesn't work as well as we might expect, because there are so many potential connections that
722 our standard statistical tools generate less than useful results.

723 The reason is that with such rich data, you can easily uncover misleading or unactionable
724 correlations. For instance, lets imagine we discover that people who are unusually active are
725 more likely to get the flu. This is a real example: when we examined the minute-by-minute
726 behavior of a small university community a real-time flow of gigabytes per day for an entire
727 year we noticed that an unusual level of running around often predicted onset of the flu [9].
728 But if we can only analyze the data using traditional statistical methods, we have the problem
729 of discerning why this is true. Is it because the flu virus makes us more active in order to spread
730 itself more quickly? While it is more likely that interacting with many more people than usual
731 makes you more likely to catch the flu, you can't be sure that this is the true cause based on
732 the real-time stream of data alone.

733 The point here is that normal analysis methods don't suffice to answer these sorts of ques-
734 tions, because we dont know all the possible alternatives and so we cant form a limited, testable
735 number of clear hypotheses. Instead, we need to devise new ways to test the causality of connec-
736 tions in the real world. We can no longer rely on laboratory experiments; we need to actually
737 do the experiments in the real world, typically on massive, real-time streams of data.

738 11.1 Research on Design and Deployment of Big Data Systems

739 In order to acheive low risk, high value outcomes efficiently, design and deployment of the coming
740 global wave of big data systems should apply top current research. To understand and address
741 the unique problems and prospects associated with big personal data, the relevant context must
742 be identified and corresponding rules-driven capabilities must be designed into the underlying
743 systems.

744 People and/or systems can determine the right rules to apply to data when the right infor-
745 mation is reliably attached to or logically associated with that data in a standard manner. Any
746 system that can make, use, receive or share big data must be capable of associating provenance

747 and purpose for all data in a common and actionable manner. Requiring a lot of narrative
748 documentation and background about the nuances and circumstances surrounding every data
749 set is both impractical and counterproductive. By contrast, a small amount of metadata listing
750 or reliably linking the parties, transactions, systems and provenance of the data would suffice.
751 This relevant context together with the data forms the basis for accountable analysis on big
752 personal data.

753 It is important for science and research to develop further solutions and options ensuring
754 contextually appropriate rules can be applied by big data systems. For rules to be effectively
755 applied, systems must not only be able to establish which rules apply but also support the right
756 functional capabilities and have appropriate information structure, format and meta-data.

757 Some capabilities will likely be essential to all big data systems, such as highly scalable
758 active storage, standard methods for integration with other big data systems and a processing
759 architecture enabling high speed statistical analytics. But there are and will continue to emerge
760 multiple types of big data systems. Some functions or controls will likely be important - or
761 even feasible - only for certain types of future systems. For instance, it is reasonable to expect
762 some systems will specialize in enormous volumes of entirely non-personal data from many real-
763 time sources (e.g. for soil science, materials engineering, astronomy, etc) while other big data
764 systems will hinge upon mass quantities of highly sensitive personal information (e.g. for clinical
765 medicine, education and life-long learning, social entertainment, etc).

766 While some capabilities, such as ingesting and processing astronomical data-sets, will be
767 unique to only a subset of big data systems it is reasonable to anticipate that data will be
768 increasingly cross-tabulated, merged and otherwise shared with other systems and data. It can
769 be nearly impossible to conclusively predict for the entire life of a system what data will be
770 received by, created in or transmitted from that system at the design phase. This prediction is
771 all the harder to make when the systems are intended for big data.

772 The four contextual facets of people, interactions, technology and data provide a sound
773 underpinning for the design of new big data and web 2.0 systems. The existing systems design

and development processes of establishing business cases, use cases, agile stories, functional requirements, etc. do not reliably identify the factors most relevant to use of big data, especially in a web 2.0 massively distributed environment. The four facets can also be used to analyze appropriate, required or prohibited uses for existing big data systems. However, it can be difficult to extract the relevant information from or apply any effective control on systems used for big data but designed to achieve limited purposes in hierarchical closed environments.

Big data, by its nature, represents a new set of business, legal and technical capabilities and requirements. Most of the worlds systems today are not capable of ingesting, storing, using or dynamically flowing big data with other systems. Considering that a) big data is of high value immediately and higher value in the short and long terms, and b) the young but competitive marketplace of big data system components, platforms, applications and other solutions is a hotbed of innovation it can be predicted that a transition to big data systems will continue. The key observation is that virtually all big data systems have yet to be designed, implemented, customized or deployed. Institutions that are the current early adopters of todays big data system will soon replace those systems and the rest of the world will adopt big data systems in phases over time. Based upon this observation,

11.2 Research on Big Data for Design of Institutions

Using massive, live data to design institutions and policies is outside of our normal way of managing things. We live in an era that builds on centuries of science and engineering, and the standard choices for improving systems, governments, organizations, and so on are fairly well understood. Therefore our scientific experiments normally need only consider a few clear alternatives (i.e., plausible hypotheses).

But with the coming of big data, we are going to be operating very much out of our old, familiar ballpark. These data are often indirect and noisy, and so interpretation of the data requires greater care than is usual. Even more importantly, a great deal of the data is about human behavior, and the questions are ones that seek to connect physical conditions to social

800 outcomes. Until we have a solid, well-proven and quantitative theory of social physics, we wont
 801 be able to formulate and test hypotheses in the way we can when we design bridges or develop
 802 new drugs.

803 Therefore, we must move beyond the closed, laboratory-based question-and-answering pro-
 804 cess that we currently use and begin to manage our society in a new way. We must begin to
 805 test connections in the real world far earlier and more frequently than we have ever had to do
 806 before, using the methods my research group and I have developed for the Friends and Family
 807 study or the Social Evolution study. We need to construct Living Laboratories communities
 808 willing to try a new way of doing things or, to put it bluntly, to be guinea pigs in order to test
 809 and prove our ideas. This is new territory and so it is important for us to constantly try out
 810 new ideas in the real world in order to see what works and what doesnt.

811 An example of such a Living Lab is the ‘open data city just launched by one author (Pentland)
 812 with the city of Trento in Italy, along with Telecom Italia, Telefonica, the research university
 813 Fondazione Bruno Kessler, the Institute for Data Driven Design, and local companies. Impor-
 814 tantly, this Living Lab has the approval and informed consent of all its participants they know
 815 that they are part of a gigantic experiment whose goal is to invent a better way of living. More
 816 detail on this Living Lab can be found at <http://www.mobileterritoriallab.eu/>

817 The goal of this Living Lab is to develop new ways of sharing data to promote greater civic
 818 engagement and exploration. One specific goal is to build upon and test trust-network software
 819 such as our openPDS (Personal Data Store) system . Tools such as openPDS make it safe for
 820 individuals to share personal data (e.g., health data, facts about your children) by controlling
 821 where your data go and what is done with them.

822 The specific research questions we are exploring depend upon a set of personal data services
 823 designed to enable users to collect, store, manage, disclose, share and use data about themselves.
 824 These data can be used for the personal self-empowerment of each member, or (when aggre-
 825 gated) for the improvement of the community through data commons that enable social network
 826 incentives. The ability to share data safely should enable better idea flow among individuals,

827 companies, and government, and we want to see if these tools can in fact increase productivity
 828 and creative output at the scale of an entire city.

829 An example of an application enabled by the openPDS trust frame work is sharing of best
 830 practices among families with young children. How do other families spend their money? How
 831 much do they get out and socialize? Which preschools or doctors do people stay with for the
 832 longest time? Once the individual gives permission, our openPDS system allows such personal
 833 data to be collected, anonymized and shared with other young families safely and automatically.

834 The openPDS system lets the community of young families learn from each other without
 835 the work of entering data by hand or the risk of sharing through current social media. While
 836 the Trento experiment is still in its early days, the initial reaction from participating families is
 837 that these sorts of data sharing capabilities are valuable, and they feel safe sharing their data
 838 using the openPDS system.

839 The Trento Living Lab will let us investigate how to deal with the sensitivities of collecting
 840 and using deeply personal data in real-world situations. In particular, the Lab will be used as a
 841 pilot for the New Deal on Data and for new ways to give users control of the use of their personal
 842 data. For example, we will explore different techniques and methodologies to protect the users
 843 privacy while at the same time being able to use these personal data to generate a useful data
 844 commons. We will also explore different user interfaces for privacy settings, for configuring the
 845 data collected, for the data disclosed to applications and for those shared with other users, all
 846 in the context of a trust framework.

847 References

- 848 1. et al JW (2009) Preparing for china’s urban billion .
- 849 2. Eagle N, Pentland A (2006) Reality mining: sensing complex social systems. Personal
 850 and ubiquitous computing 10: 255–268.

- 851 3. PENTLAND A (2009) Reality mining of mobile communications: Toward a new deal on
852 data. The Global Information Technology Report 2008–2009 : 1981.
- 853 4. Pentland A, Lazer D, Brewer D, Heibeck T (2009) Using reality mining to improve public
854 health and medicine. Stud Health Technol Inform 149: 93–102.
- 855 5. Singh VK, Freeman L, Lepri B, Pentland AS (2013) Classifying spending behavior using
856 socio-mobile data. HUMAN 2: pp–99.
- 857 6. Pan W, Altshuler Y, Pentland AS (2012) Decoding social influence and the wisdom of
858 the crowd in financial trading network. In: Privacy, Security, Risk and Trust (PASSAT),
859 2012 International Conference on and 2012 International Confernece on Social Computing
860 (SocialCom). IEEE, pp. 203–209.
- 861 7. Greene K (2008) Reality mining. Technology Review .
- 862 8. Kuneva M (2009). Roundtable on Online Data Collection, Targeting and Profiling .
863 http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm.
- 864 9. Madan A, Cebrian M, Lazer D, Pentland A (2010) Social sensing for epidemiological
865 behavior change. In: Proceedings of the 12th ACM international conference on Ubiquitous
866 computing. ACM, pp. 291–300.
- 867 10. Pan W, Ghoshal G, Krumme C, Cebrian M, Pentland A (2013) Urban characteristics
868 attributable to density-driven tie formation. Nature communications 4.
- 869 11. Grossman L (2009) Iran protests: Twitter, the medium of the movement. Time Magazine
870 17.
- 871 12. Barry E (2009) Protests in moldova explode, with help of twitter. New York Times 8.
- 872 13. World Economic Forum (2011). Personal Data: The Emergence of
873 a New Asset Class. Available on [http://www.weforum.org/reports/](http://www.weforum.org/reports/personal-data-emergence-new-asset-class)
874 personal-data-emergence-new-asset-class.

- 875 14. Lima A, Domenico MD, Pejovic V, Musolesi M (2013) Exploiting cellular data for disease
876 containment and information campaigns strategies in country-wide epidemics. School
877 of computer science university of birmingham technical report csr-13-01, University of
878 Birmingham.
- 879 15. Narayanan A, Shmatikov V (2008) Robust de-anonymization of large sparse datasets. In:
880 Security and Privacy, 2008. SP 2008. IEEE Symposium on. IEEE, pp. 111–125.
- 881 16. Sweeney L (2000) Simple demographics often identify people uniquely. Health (San Fran-
882 cisco) : 1–34.
- 883 17. David Tacconi PLBACSGT Oscar Mayora, Haring C (2008) Activity and emotion recog-
884 nition to support early diagnosis of psychiatric diseases. IEEE, pp. 100-102.
- 885 18. de Montjoye YA, Hidalgo CA, Verleysen M, Blondel VD (2013) Unique in the crowd: The
886 privacy bounds of human mobility. Scientific reports 3.
- 887 19. Song C, Qu Z, Blumm N, Barabási AL (2010) Limits of predictability in human mobility.
888 Science 327: 1018–1021.
- 889 20. Bilton N girls around me: An app takes creepy to a new level. The New York Times .
- 890 21. United States Environmental Protection Agency (2007).
891 RCRA Corrective Action Institutional Controls - glossary.
892 <http://www.epa.gov/epawaste/hazard/correctiveaction/resources/guidance/ics/glossary1.pdf>
893
- 894 22. DeMeo RA, Doar SM (2011) Restrictive covenants as institutional controls for remediated
895 sites: Worth the effort? The Florida Bar Journal 85.
- 896 23. Juniper Networks (2012) Secure data access anywhere and anytime: Current landscape
897 and future outlook of enterprise mobile security. Forrester report, Forrester.

- 898 24. Florida Department of Environmental Protection - Division of Waste
899 Management (2012). Institutional Controls Procedures Guidance.
900 http://www.dep.state.fl.us/waste/quick_topics/publications/wc/csf/icpg.pdf.
901
- 902 25. Center for Environmental & Human Toxicology University of Florida (2005) Development
903 of Cleanup Target Levels (CTLs) For Chapter 62-777, F.A.C. Technical report, Division
904 of Waste Management Florida Department of Environmental Protection.
- 905 26. United States Environmental Protection Agency (2005). Institutional Controls Bibliog-
906 raphy. <http://www.epa.gov/superfund/policy/ic/guide/biblio.pdf>.
- 907 27. United States Environmental Protection Agency (2012) Institutional Controls: A Guide
908 to Planning, Implementing, Maintaining, and Enforcing Institutional Controls at Con-
909 taminated Sites. Technical Report OSWER 9355.0-89 EPA-540-R-09-001, EPA.
- 910 28. (2013) User-Managed Access (UMA) profile of OAuth2.0. Technical report, Kantara Ini-
911 tiative.
- 912 29. (2013) Binding obligations on User-Managed Access (UMA) participants. Technical re-
913 port, Kantara Initiative.
- 914 30. Barber S, Boyen X, Shi E, Uzun E (2012) Bitter to Better – how to make Bitcoin a better
915 currency. In: Proceedings Financial Cryptography and Data Security Conference (Lecture
916 Notes in Computer Science Volume 7397). pp. 399-414.
- 917 31. Stalnaker S (2013). The Ven currency. [Http://www.ven.vc](http://www.ven.vc).