Today after the thousands of years of human struggle including our American journey, we are only 66 years after
the Universal Declaration of Human Rights was adopted in reaction to the horrific human tragedies of WWII. For
these scant 6 plus decades, human life was seen as whole and based on an essential emergent and commonly held
human dignity. Today this human whole and dignity has been fractured, through information science and
cyberspace into myriad bits sometimes called data or attributes of human life. This fracturing has been motivated
and inspired by the incredible value of human attributes in commerce to those that collect, aggregate, store and
analyze human attributes; partnered with a reluctance to ensure that revenues are fairly handled; and not
commercially unjustly favoring some members of cyberspace over others. Nowhere is this truer than in the setting
of big data. Human rights, individual human rights, largely the glue of democratic countries, have no or little
standing in this fractured world. What kind of rights does a person’s hair color have or my disembodied shopping
pattern? Much of this disconnection of human rights and human attributes has been created by design. After all,
cyberspace is largely a creation of human beings. But this creation of commercial wealth through the monetizing of
human attributes on the internet and cyberspace is devolving now into something fundamentally inequitable, and
it is simply unnecessary. This is urgently not the best outcome for life on earth. Privacy, a somewhat new,
emergent and still ill-defined concept is currently a lonely outpost to stand up to this challenge. I have been
working for the last two years in the NSTIC Identity Ecosystem Steering Group (IDESG). The IDESG has yet to be
able to acknowledge the extent to which our current effort incentivizes the inequitable commercialization of
human attributes. Under the auspices of the National Program Office our Department of Commerce is creating a
burdensome and complex system in an effort to preserve privacy without allowing discussion in tractable terms of
its essential trustworthiness; especially in regards to the fair handling of the wealth of human attributes. I have
heard repeatedly that without these inherently unfair incentives commercial entities will not participate in these
privacy preserving efforts. With these commercial cultures being supported and reinforced by nations and
governments, while ignoring the human rights supported by the culture-at large, we may be devolving into a chaos
of inequity.

Why is the vast wealth of human attributes not benefiting human lives here and now? What is needed to find a
better way forward?

One of the chief dilemmas for cyberspace and online networked environments is the lack of anonymity. A certain
degree of anonymity underpins and is required to insure civil liberties and the over-reaching of the state. Progress
must be made in constructing this possibility but my intention here is to show that it is this very fact of the
inherent specificity of human behavior and identity in information systems that hold the promise of another way
forward. A number of us are working urgently in this very area. This lack of natural anonymity means that the
identity of just about every human act, in motion, online and in cyberspace is known. Our challenge is to know
what to do with this fact.

What is needed to liberate the positive benefits of this fact?

There are not enough trustmarks in the world to create trust in this current inequitable environment without some
fundamental adjustments in organization design through the science of organizations, capability enhancing
information architecture and metadata, the science, neurology and psychology of trust, welcoming art of embedding a user experience of human dignity and rights along with major innovations in democratic governance.

Only a multidisciplinary approach is appropriate to address this problem of “responsible use”. Methods of “encoding privacy policies in machine-checkable forms and ensuring their compliance and auditability; managing the collection, retention, and dissemination of sensitive data; and ensuring the confidentiality and integrity of sensitive data, while enabling desired uses of them” are possible and may be useful for ensuring privacy. This will not overcome the ultimate incoherence and dilemma of whom and how are these systems going to be certified—how many layers of certification are enough? Who is the ultimate certifier and how will they be trustable? While many of these efforts are laudable and undertaken for good purpose today we have a deficit of trust that cannot be solved with increased complexity. Instead we see the world becoming less stable and less governable through complexity.

We need to:

1. Re-establish the respect and dignity of life-with-rights as the central purpose of information systems, information architecture and cyberspace.
2. Create an informed valuation for human attributes that is openly available and based on a reliable currency that all parties to interactions have access to and can serve as the monetary basis of cyberspace commerce.
3. Begin networked interactions online and in cyberspace with an agreement, perhaps call it a Memorandum of Social Cooperation that establishes fair ground rules for transactions online and in cyberspace where the revenues from human attributes in interactions is divided fairly. This valuation can be assisted through automation.
4. Build fair markets based on these practices.