Opening Statement by Dennis Jennings on the
General Scheme of the Data Sharing and Governance Bill
23rd May 2017

Thank you Chairman and members of the Committee for the opportunity to meet you to discuss the provisions of the General Scheme of the Data Sharing and Governance Bill.

I would like to introduce myself. My name is Dennis Jennings. I have a background in technology, computing and communications. I headed up the Computing Services in University College Dublin for 22 years. I am an Internet Pioneer, having made significant contributions to the development of the global Internet in the 1980's. More recently I am early stage investor and non-executive director. I also serve on the Open Data Governance Board of the Department of Public Expenditure and Reform.

It is evident that the modern State requires personal information to run effectively and efficiently and to support the individual citizen and resident. It is also evident that as citizens, we expect more of state services than ever before. We expect them to be efficient, timely, cost-effective and fraud-free, and driven by automated processes. But we also expect to be protected and safe when we use state services. Part of this safety is the protection of our privacy and our personal data.

When I read the draft Bill last year, I was shocked and disappointed. But it stimulated me to consider the Principles that should underpin a shared e-infrastructure that would enable the public sector to properly serve the citizens of the state. A copy of the current version of my paper entitled "**Implementing Public Service Shared e-Infrastructure: The Individual & the Irish State – The Grand Bargain**" has been submitted to the Committee.

My paper outlines the ten principles that I believe should be adopted <u>before</u> the implementation of any shared Stats/Citizen e-infrastructure is even contemplated.

I'd like to focus my comments on some of the issues highlighted in my paper.

Identity and Opt-in.

Little can be done to implement an appropriate shared services e-infrastructure without agreement – I stress agreement – on a unique, rigorously authenticated, biometrically and multi-factorial secured identity mechanism for each individual.

Current identity mechanism – Passports, Driving Licenses, Medical Cards (GMS & PPSN), Public Services Cards (PPSN) – are all, in my view, poor substitutes for what is actually required.

General buy-in to the use of unique identifiers can and will be achieved by the State offering compelling value propositions, better, faster, slicker, more convenient, more accurate, more efficient services, so that in due course, when public confidence in the data protection provided by the systems has been established, the identification system may be made compulsory.

The State and Civil Society organisations, representing the individual's rights to Data Privacy, need to agree on the necessary identity approach and solutions.

The current situation where the Department of Public Expenditure and Reform is trying to introduce 3 million Public Services Card, using data sharing from multiple sources under the provisions of a very old and out-of-date (from a privacy perspective) Social Welfare legislation is, I think, truly shocking, and a gross breach of this principle and of the trust that is required.

Queries/Responses through Data Access NOT Data Sharing

A fundamental principle to be adopted in any shared services e-infrastructure implementation is that individual personal data is NEVER copied and shared, with consequential loss of control over access and of authenticity, but is ALWAYS accessed dynamically on-line. In addition, no general access to the underlying data may be given, rather such access is provided so as to respond with answers to a pre-defined, and approved, set of queries.

In my view the data sharing concept underlying the Bill is fundamentally flawed.

Authentication and Access

To ensure confidence in the new shared services e-infrastructure, access to personal data held by the State must be restricted (a) to the individual data subject and data owner, and (b) only to legally authorised (and EU GDPR compliant) organisations / personnel, and strict multi-factorial authentication of all individuals with query access must be required.

The Bill is almost silent on the need for rigorous authorisation and authentication of every person in the public service that has access to data – and this, I believe, is a major defect.

Data Logging by Requestor, Responder, and Centrally

It is also self evident that all access to personal data must be logged and recorded, so that audits can be undertaken, and so that individual citizens can easily track by whom, why and when their personal data has been accessed. Both the requesting and the responding organisations' data privacy gateways must automatically log an encrypted hashed record of all queries and data requests, and resulting responses, that access data relating to an individual.

The Bill has no mention of the data access logging that is a central component of a trusted shared e-infrastructure.

Secure on-Line Portal for Individuals

A vital part of any shared services e-infrastructure is the Citizens' portal, where citizens and residents can track the State services provided and the details of the use and access to their data.

The Bill has the briefest mention of a "Single Customer View" and future on-line authentication. That is ridiculous, because citizen access to their own data must be an integral part of any implementation from the very beginning.

The Bill needs a lot of work.

Thank you.