7. **NSA:** for the foreseeable future, NSA has two separate definitions of what constitutes content based on EO 12333 and FISA/PAA collection. FISA considers communications data to be part of the content of the communication, hence FISA has no separate concept of metadata. All discussions at the conference were therefore **focused on "standard" collection under the authority of EO 12333.**

8. There is a constitutional expectation of privacy within the US. For communications data this is harder to quantify than for content. New procedures will permit a differentiation between content and communications data allowing for far greater data usage and advancing other related changes. A tension remains between the desires to minimise shared data containing US identifiers, and engaging more openly to support the foreign cryptologic mission.

9. It is harder to define what constitutes a US identifier with DNI data - where unclear it is treated as US. NSA is moving from minimised records within their databases to minimising identifiers within reports. Sharing unmasked US identifiers with second party SIGINT partners will be easier than with some US domestic partners.

10. **All:** All SIGINT agencies seek to protect their equities, especially relating to Special Source Exploitation (SSE.)

11. Special categories of data were considered in the context of their potential to contribute to pattern of life analysis. An increasing amount of new data types are available to SIGINT agencies, some proving difficult to categorise as either content or communications data. The conference agreed to step back from trying to categorise the data and simply to focus on what is shareable in bulk.

12. Consideration was given as to whether any types of data were prohibited, for example medical, legal, religious or restricted business information, which may be regarded as an intrusion of privacy. Given the nascent state of many of these data types then no, or limited, precedents have been set with respect to proportionality or propriety, or whether different **legal considerations applies to the "ownership" of this** data compared with the communications data that we were more accustomed to handle. It was agreed that the conference should not seek to set any automatic limitations, but any such difficult cases **would have to be considered by "owning"** agency on a case-by-case basis.

(comment: NSA normally considers any target data (pattern of life or other) that can **be characterized as** "foreign intelligence" as proper for collection, analysis and production.

Comment [redacted]: Page: 3
[redacted] used the term "off limits".

35. **(d) ICREACH:** Sstill a pilot, this provides minimised DNR data to Sigint-cleared and appropriately trained analysts across the US Intelligence community. Second Party derived data is currently not made available to US Intelligence Community (IC)(domestic)domestic agencies (although GCSB has agreed that theier DNH metadata may be shared), but such data would be valued. In the hope that such agreement will be forthcoming, NSA has persuaded other US IC agencies to make almost 100 bn previously NOFORN records shareable with the 5-eyes via GLOBAL REACH. VoIP is treated as DNR though with only DNR records and fields shown to analysts. Making DNI available through ICREACH is currently restricted due to limited automated (general counsel approved) methods toprevented by US policy on minimize DNI metadata.ation.

Comment [redacted] Page: 6
The 'US' was implicit in this statement but not voiced at the time.

36. **'Deconfliction' is not formalised through ICREACH. Query records can potentially** be used to alert analysts that other analysts are looking at the same data. Deconflicting operations remains a tough challenge requiring increased coordination of operations and collaboration.

37. There is interest in the relationship between the implementation of A-SPACE (a U.S. DNI initiative to link all U.S. IC analysts to common tools, and sharable databases and allow for greater collaboration) and ICREACH inasmuch as it may **affect Second Parties' internal procedures and access issues with domestic** agencies.

38. **(e) U.S. NSCID5:** This is a specific method of NSA providingsharing uniminimized SIGINT data to CIA (as if CIA had collected it itself) **in support of the latter's** operational mission., and dData from Second Parties is shared with CIA in accordance with special agreements between NSA and each second party.

39. GCHQ are employing methods (a) and (b). For military SIGINT needs GCHQ **uses GCO's**[1] to reach back to UK and 5-EYES **repositories. The military's work** within the ambit of the National SIGINT Organisation comes under the authority of GCHQ.

40. NSA shares US SIGINT data with all US SIGINT elements that operate under DIRNSA's operational control.agencies. With Second Parties there is an initial minimisation of the data when possible; however all second parties have agreed to abide by U.S. minimization criteria., Ffor US intelligence agencies NSA mustthere is further minimizesing of the data, before sharing and for other US agencies (such as law enforcement) NSA only provides data under its "technical support" mission. Currently, all such data is minimized before sharingthere is another, further level of minimising of data (most restricted data set.)