Institute for the Secure Sharing of Online Data: Technical support

John L Manferdelli

The social impact of “fake news,” political targeting, manipulative advertising and erosion of historically stable social norms has been dramatically changed by internet interactions. Internet mediated communication has changed where and how people work, how they relax, how they learn, how they purchase and how they engage in structured and unstructured social and business activities subtly and sometimes, not so subtly, changing formerly well-understood patterns of behavior. These interactions are novel not just because of real-time access to information but the consequentially enabled automated information operations which have resisted the normal defenses of social dialog and critical thinking. In some ways, the social upheaval caused by the internet is analogous to the effect of new mass market communications technology like radio and television which were leveraged by national socialist movements prior to World War II or, earlier still, newspaper propaganda fueling nationalist fervor for the Spanish American war. Internet technology has dramatically changed the scale and customization of opinion forming communications. Just as automation gave rise to these changes, response and understanding may well be rooted in new information technology which can analyze these new trends using large scale analysis of unstructured social data to give much needed insight.

Our goal here is ultimately to guide the design and operation of the technical infrastructure for the storage, use, curation, distribution and analysis of this critical data. However, designing infrastructure requires some thought as to policy goals for use of the data and this requires some speculation on the desiderata for the policy objectives of such an infrastructure. These should include:

1. The ability to store and efficiently retrieve large amounts of structured and unstructured data, petabytes of original data.
2. The ability to ensure availability of the data on demand and the recovery of the data in the event of malfunctions, “insider” errors and even malign intent from some insiders and robustness in the face of physical catastrophes.
3. Reliable curation of data from source provenance through correction of errors and updates based on subsequent information.
4. Confidentiality of data, preventing authorized use and data integrity, preventing corruption of the source data.
5. Audit logs that can track data access and reveal subtle misuse or unauthorized access.
6. Audited, certified removal of data that must be withdrawn because of defects or legal process.
7. Clear standards and procedures for releasable data analysis.
8. Strong authentication of subject users to prevent unreasonable access due to stolen credentials.

9. Processing standards that prevent subject users from introducing vulnerabilities into the processing infrastructure.
10. Processing infrastructure allowing computationally intensive use of the data.
11. Possibly standardized but continually evolving analysis tools to ensure accuracy and cross calibration of results.
12. The ability to automatically provided differentiated policy enforcements for a wide variety of data sets from a wide variety of suppliers who may uneasy about other providers, users or attribution.
13. The ability to respond, if required, to lawful requests for data production as well as procedures to prevent abuse.
14. Technical mechanism to "verify" results which do not interfere with protected researcher ideas, materials or experiments.
15. Development of tools and techniques to measure data accuracy and fidelity.

A key characteristic affecting provenance, protection and removal of data will be the subject matter of the collections. The subject matter may adversely affect individuals by inadvertently disclosing individual opinions, characteristics or circumstances. Individual or composed data sets to reveal illegal or protected behavior and as a result, the revelations may subject people or groups to oppressive sanctions. Nation state restrictions on data (e.g.- the "right to be forgotten," data locality) may be triggered depending on subject matter affecting oversight and operations.

The infrastructure should not only guard against misuse but promote new insights based on persistent development of new techniques and procedures that endure after individual projects terminate.

Confidentiality and integrity generally

All data collections should be encrypted in storage and transmission and protected from eavesdropping during use. All original data sources should have cryptographic integrity protection against deliberate or accidental modification or corruption.

Encryption and integrity protection should be sufficiently robust so that any such lost encrypted data poses no threat and recovery of potentially modified data sources can be cryptographically verified as to integrity.

A concomitant requirement is the production, storage, use and availability of cryptographic keys. These should all be subject to the multi-actor approval for critical tasks.

Labelling, taint tracking, audit and curation

Sufficiently descriptive metadata should be maintained and augmented to provide non-repudiatable provenance, accuracy annotations, modification history, subject matter designations and special terms and conditions affecting use. Use of data should be securely logged and the technical infrastructure should allow a complete inventory of data used in any

given analysis. Cryptographically secure mechanisms should be employed to tract the users and programs affecting any such analysis. These capabilities can be used not only to support research conclusions in an automated way but to identify errors or misuse even after the analysis is complete.

Multi-actor approval requirements for critical tasks and administrative access generally

As a side effect of labelling, data sources should be identified. Any critical tasks like changing source data, manipulating or revealing cryptographic keys, deletion or modification of logs and data deletion should be subject to an authorization regime that requires multiple authenticated authorized parties to consent to the action prior to execution without exception and those activities should themselves be subject to strict logging and auditing.

Storage and backup

Original data should be encrypted, integrity protected and replicated to protect against failure of individual storage devices, transmission facilities or even processing centers. Storage replication should apply equally to audit information and logs.

Corrections, removal

A difficult to implement, but important capability is the ability to provide absolute assurance that data subject to deliberate and permanent removal is, in fact, unrecoverable. This will be especially important as it pertains to legal process, individual privacy and misuse of surviving data that may affect basic human rights. Certified removal should be subject to multi-actor approval for critical tasks.

Authentication of users and programs

A pre-condition for protecting against unauthorized use of data, especially sensitive data, is verification of individual users and programs accessing data. Authentication techniques should be sufficiently robust to prevent continued misuse of compromised credentials. Authorization should, at a minimum include a secure audited and maintained hardware token and not merely passwords.

Authorization

Different data sets should be made available to different users under a potentially complex set of access rules which may include time based restrictions, restrictions affecting use in conjunction with other data sets (which may, in combination, reveal restricted information). Mechanisms for expressing such rules, in a machine enforceable manner will need to be developed along with software “guards” which enforces such rules.

Auditing use

The most diligent application of the foregoing mechanisms cannot prevent unforeseen errors or vulnerabilities suspected after data use. Audit logs for critical activities and data access can limit the adverse effects of breaches or errors and help determine the nature and extent of such breaches and errors.

Processing and streaming

It is natural to expect that organized and ongoing data analysis will provide the opportunity for the development of reliable and innovative tools to ingest, transform, tally, assess and analyze data. While most data analysis employs tools that are discarded or poorly maintained, an institute can provide a unique opportunity for innovation and quality for commonly needed tools (even before the common need is recognized). A clear benefit for researchers is access these tools and methods.

Review of results

Because the underlying data can be restricted and may reveal information that should not be disclosed or may lead to erroneous conclusions, a careful review of the results would be useful. Automatic tracking of data sources and methods greatly automates any review procedure.

Restrictions based on copyright, trade secret, defamation, insider trading

Data use may unknowingly lead to violating restrictions on data based on copyright, trade secret, defamation, insider trading, national laws or individual privacy restrictions. While technical infrastructure cannot automatically prevent these dangers. The infrastructure can accelerate and inform mitigating responses. An interesting area of research for which ISSOD is opportunistically positioned is privacy preserving analytics. Based on homomorphic encryption and differential privacy the Institute can develop tools which process data obliviously, that is, in a manner where only conclusions are revealed while underlying data remained provably private. Alternatively, hardware isolation and hardware assisted cryptographic techniques can be employed to assure, given adequate program characterization, that, only aggregate and conclusory information is disclosed while, again, underlying data and personally identifiable information remains provably private. This technique can be extended so that data sources can be combined, kept secret and yet processed in a manner that provides fused analysis from data sources which would ordinarily be too sensitive to use in conjunction.

Diligence to prevent data poisoned analysis, propaganda

Poisoned data can destroy the efficacy of large scale data analysis and may even result in the promotion of propaganda based on false and misleading data. An institute like ISSOD can develop tools to detect poisoned data and faulty data that may result in erroneous conclusions. Individual projects can seldom devote the effort to develop and maintain such tools. These tools themselves provide a separate and important area for research.

In conjunction with these tools, ISSOD provides an environment for “red teaming” data access, use and analysis and can help develop mechanisms to detect and prevent adversary manipulation of data and results.

A new hope

Capable technology infrastructure is an important aspect of enabling using new information sources to gain insight and it can overcome both real and imagined objections to use of this new and critical resource.