G. Describe how the innovation consumes data (as input), produces data (as output), and/or transforms data.

Email is primarily a producer of data, and this is one of its important characteristics. Email produces data that is human communication - the messages. Messages contain both data: the text and other media being communicated; and meta data: the sender and recipient email addresses, subject, data/time, and other SMTP-required meta data. It is important because email is the most naturally archived (stored) form of human communication. Physical mail, voicemail, texts, etc can be stored data, but are typically stored in ad hoc rudimentary ways such as simple lists or files. Email servers typically store all messages by default and email clients provide ways to manage the stored data such as search capabilities and filters. This ability to store communication and manage it as data is one of the reasons email is as widely used as it is. People and organizations use email as a record of communication in legal proceedings and to recall details of what has been communicated.

In some sense email also transforms data. Email attachments exist as electronic data and then are transformed by email to another form of data (the attachment) for delivery and storage in the email system.

H. Describe at least one data storage concern, data privacy concern, or data security concern related to the innovation.

Email being the best form of archived human communication data also raises privacy concerns. Just as well-stored communication is good as a record of what has been communicated, this stored data when possessed by unintended people can be a privacy violation. The lifetime of an email message introduces privacy concerns in each phase of its existence. The message is often stored in a folder in the email client on both the devices that were used to compose the email and to read it. If either device falls into unintended hands, the privacy of the message may be compromised. Email is communicated over the public Internet which, due to its use of open protocols and routing, is susceptible to unauthorized people sniffing the message while on the network. Encrypted email can mitigate this concern, but many email clients still don't encrypt messages by default. The message is also often stored both on the sender's email server and on the recipient's email server. These servers can be accessed by employees of the companies, by hackers who get in to the servers, and by law enforcement (with subpoena or warrant) - again exposing private communication to outside parties.