A Minor Pitfall in the Telnet Protocol

Designers of Telnet options should be aware of the following possible
case in the Telnet protocol which may generate unexpected behavior on
either end of the connection. Although at present none of the existing
options are susceptible to this problem, it could arise in the future.

The Telnet sync sequence causes all data to be deleted from the data
stream until a data mark is encountered. Telnet control functions are
not affected by the sync sequence (see page 9 of the protocol
specification). A Telnet option subnegotiation could be defined such
that it had an affect on the data following it in the data stream. For
example, a subnegotiation might be used to indicate the terminal was to
display the following data in a particular font or should receive other
special treatment by the terminal. A Telnet sync sequence sent after
such a subnegotiation and its data and before the subnegotiation had
been processed could resuit in the subnegotiation having its affect on
data other than that intended.

Two possible solutions come to mind at once. First, the data to be
affected could be included as a parameter of the subnegotiation. in
other words, the data is inserted in the data stream before the IAC SE
that terminates the subnegotiation. The disadvantages of this solution
are both theoretical and practical. Theoretically, it is improper and
not really in the spirit of the Telnet protocol design to send data as
subnegotiation parameters. Practically, in a situation where this case
would arise it would be equally unexpected behavior (and perhaps
confusing if a human was affected) if all data except that affected by
the subnegotiation was flushed.

The second solution would be for designers of options which have such
subnegotiations define a subnegotiation or other mechanism that would
follow immediately after the Data Mark and nullify the affects of any
offending subnegotiation. The exact semantics of such a subnegotiation
would probably be very specific to the option.