illustrates the power that system administration staff have to gather and release private data. Hackers, or unauthorized persons, may also have access to stored data and thus are always a looming threat to safely securing data that resides on an Internet server. This threat is twofold: accessing and making public data that is collected or destroying data through distributed viruses. E-researchers will need to advise the participants that they cannot absolutely guarantee that data will not be accessed, used, changed, or destroyed by others. They will also need to provide details outlining the steps they are taking to attempt to provide privacy, confidentiality, or anonymity. Roberts (2000a) and Witmer (1998) have observed that there is sometimes a lack of understanding by both research participants and researchers with respect to the technical and storage capabilities of Internet technologies. Specifically, they note that there is an elevated "risk of exposure of the subject's identity and the potential accessibility of their per-sonal information to others" (Roberts) and, as such, the participants should be made aware of this by the researcher. At this point, the participants can make a decision to participate, or not, based on this information. Further, if the security of the data does become compromised, the e-researcher will be somewhat better protected from humil-iation, a possible ruined career, and legal action if he/she has informed the participants of this risk.

Finally, if e-researchers are dealing with sensitive data that, if made public, could bring harm to the participant, they will have to make the difficult decision of whether or not it is even ethical to use Net-based communication. The e-researcher has the option to use Net-based communication software that encrypts correspondence between researcher and subject (this software is discussed in the next chapter). E-researchers may also wish to routinely encrypt sensitive files (such as digitized audio interview transcripts) that are stored on personal or group servers. The stand-alone encryption program PGP (Pretty Good Privacy), available on the Web at no charge, encodes and decodes files, thereby protecting the privacy of files and electronic mail. A Frequently Asked Questions file explaining PGP use is available at http://cache .qualcomm.comigetpg.htm.

Another of the complexities and corresponding problems that e-researchers encounter with respect to privacy, confidentiality, or autonomy, is dealing with how to obtain informed consent from online participants. The following section provides a discussion of the issues, problems, and dilemmas facing e-researchers when obtaining consent from online participants.

OBTAINING CONSENT FROM ONLINE PARTICIPANTS

We begin the discussion of means to obtaining consent by reiterating the need for the e-researcher to gain the trust and support of all potential participants. This support can be effectively achieved in an introductory note that outlines the purpose of the research, the details of the research process, what is expected of participants, and the steps that will be taken to protect privacy and confidentiality. The box includes an example of an informed consent form at a western Canadian university.