1) Privacy really is something to be concerned about. One never knows what data about him or her is going to be used, bought and sold and with which purpose. Not only individuals who use the Internet should be worried about their information but also people who never used computers in their lives might provide relevant information to Companies.

Take for instance Health Insurance companies. This segment of industry increases its profit based on the amount of people who pay for an insurance but don't use it, that is they don't need it. Thus individuals who are of old age or sedentary are more likely to get sick and make a broader use of their insurances, which decreases the company profit, meanwhile individuals who are younger and more active are less likely to get sick and use their insurances. But how does an insurance provider acknowledge if someone is physically active or not? The company can make deals with local gyms or sport centers and buy people's information.

Nevertheless, computers and the internet have a big role in the privacy discussion because, with the advance of technology, people are constantly generating more and more data and they're also receiving more and more data. Since more and more data is being generated, more likely this data is to be used with purposes that might concern the person who generated that data in the first place. Social media for example has a big role in this matter. Nowadays most job interviewers will search on Facebook, LinkedIn and similar social network for the candidates (for that job) profiles and make an analysis of what they talk about, what they share, what pages they "like" and so on. Twitter, for instance, generates statistics over the tweets of people, which might be relevant for companies as well.

A lot is being talked about Big Data and Data Mining as well. That is, the amount of data collected by companies is so huge that new types of algorithms that seek to recognize patterns over the data are being developed. This type of information is relevant to many companies: for example, Amazon sells more if it suggests products that the consumer would be willing to buy. So based on someone's profile and based on people with similar profiles, what products should be suggested to each person? That's the type of question that Big Data and Data Mining seek to answer more and more accurately.

We live in an age where information is really relevant to companies. The more information one company has, the best decisions it'll make.

2) According to Sara Baase (A Gift of Fire - Social, Legal, and Ethical Issues for Computing Technology): “Free speech advocates argue that judges should examine the individual case and determine if the evidence is strong enough that the organization requesting the identity is likely to win a lawsuit—and only then issue a subpoena for the person’s real name.”

Which means that each case is a different case. Thus, in that situation, the candidate being “injured” might question in a judge either if the case is enough for the identity of the person using the anonymous re-mailer to be revealed.

He or she certainly cannot demand that the identity of the other person to be revealed since his or her judgment is biased. A neutral judge should analyze the case.

In my opinion, given the situation, most cases would not permit the identity of the anonymous sender to be revealed for some reasons:

- If whatever is being said is a lie the “injured” candidate can argue in favor of himself or herself. That is, he or she can prove the sender wrong.
- Freedom of speech gives the sender the right to say almost anything he or she wants.
- The “injured” candidate can use that in his or her favor by proving the content of the e-mail to be a lie and by casting doubt on the sender. That would maybe make some people conclude that the natural sender of the e-mails to be the opponent and therefore it would prejudice the opponent’s reputation.

An interesting point to question is: how is the list of supporters available for the sender in the first place? The only way for him or her to have access to that list is if the list itself has been sold or hacked which would both be ethical questionable as well.

If it was hacked, then the “injured” candidate has a case against his or her opponent. If it was sold maybe it isn’t even the case of the “injured” candidate to question his or her opponent’s ethics since he himself or her herself might have made that list available unethically.

Another point that I would highlight is that nowadays e-mails like those usually are marked as spam which still doesn’t make it ethically acceptable, but it makes it less harmful for the election itself.

But anyway, I still would reinforce that each case is singular and should be analyzed separately. Thus a judge should decide that the content of the e-mail is too harmful for the election or not.

3) In my opinion, there might be legislation defining what should or should not be received by the government, policy and similar instances.

This matter actually isn't only about communication but about science in general. Take nuclear fission for example, the technology is a great source of energy and if well used it can provide good things for society. Nevertheless, the very same technology that provides a large amount of energy can be used to produce nuclear bombs that can kill millions.

The best way to approach the issue and to prevent technology to be used for illegal purposes is to legislate over their use.

The same principle can be applied to cryptography. The technology is great if well used since it safeguards the communication and protects people's privacy, but it also provides means for unwatched criminal and/or terrorist communication.

Therefore, I think that cryptography should not be avoided, but whenever there is a case of suspicion and enough reasons for the government to request the privacy to be broken it should be broken.

A recent case happened in California where the FBI asked Apple to provide information from the iPhone of a shooter who killed some people and Apple denied arguing that they were protecting his privacy.

I can understand both sides. Apple, by trying to protect their clients' information make a good marketing for their products since people rely on the company to protect their privacy and, on the other hand, FBI trying to break in a shooter iPhone to collect information that might help to understand why he did what he did.

It's in fact a very complex situation and I think that, as in the question 2, each case is particular and should be analyzed individually. Thus, the technology should be available for people and companies to use, but it also should be reinforced by law that if there are enough reasons for the privacy to be broken (such as in criminal or terrorist acts) the provider of the technology is going to collaborate with the government, policy and so on in order to provide the relevant information for the investigation or judgement of a judge.

This point of view is actually a compromise between people being able to claim to live in a free society and the possibility of the government to make interception of e-mail communications.