Security FAQ

It's important you make sure the reporters and users of any map you build understand the risks involved:

- any SMS could be traced, and certainly could be read by the telco
- email can easily be traced and read
- Almost any input to Ushahidi could be traced, and if you're working in a hostile environment it's probably safe to assume that governments have more resources than we do, and WILL hack a deployment if they want to. You should encourage reporters not to do anything that incriminates themselves, and not to submit any identifiable details unless absolutely necessary.

Can admin erase IP and any evidence of where messages are coming in from? (I recognize that in some countries - like the UK - this is illegal)

Just had a quick search in the code and can't track down the IP related bits, so not sure what you can do with those.
However even if you can remove these from Ushahidi, it's important to realise these often end up in server logs anyway, so they might be harder to remove if you don't control the server.

In the case of SMS I note that there are suggestions to delete sent messages but in fact if people's phones are monitored or there is pressure on the telco or just because of tower pings, wouldn't it be easy to pinpoint which cellphones sent in information? Is there a secure way to use sms?

SMS can definitely be tracked by the telco. Obviously it depends on where you're operating as to how likely this is.

How you mitigate this will depend on the situation. In some countries you can get prepay sim cards without supplying any ID, so while the phone is traceable to the sim/phone number, its not traceable to the individual.
With any information you collection it is usually best only to collect the information you need. If you don't need the name of a reporter, don't collect it.

However, in cases of greater security risk, do you have suggestions for secure hosting and if SSL certificates can help or hinder data inputting...
We would recommend always using SSL with a valid certificate, even on a low risk deployment. This reduces (but doesn't eliminate) the risk of the site being hacked and details being monitored.