Is Legislation an Effective Measure to Contain Spamming ?

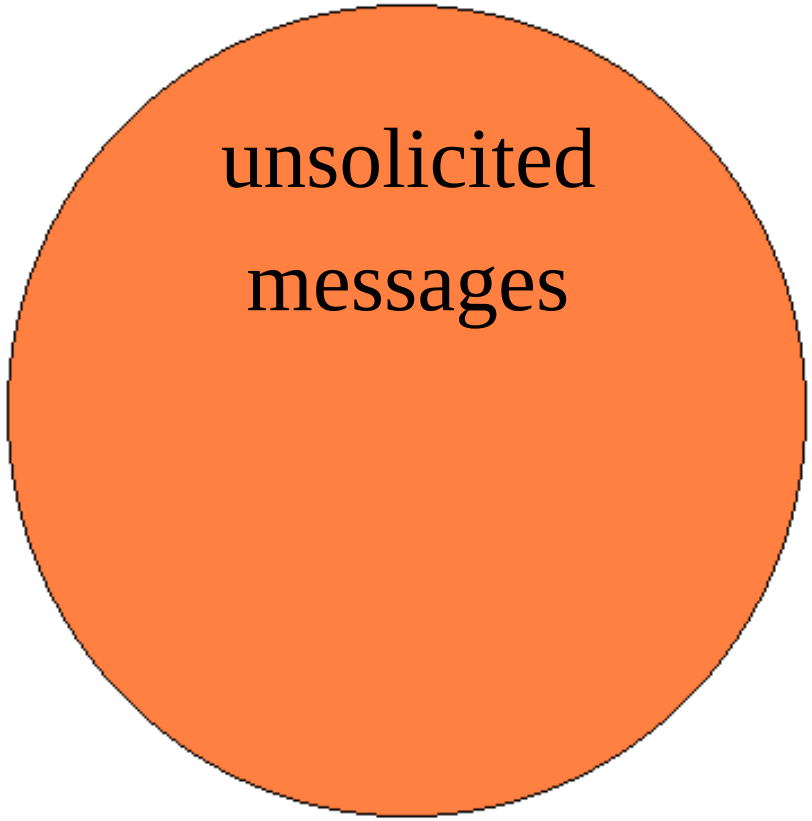
K S WONG

OFTA

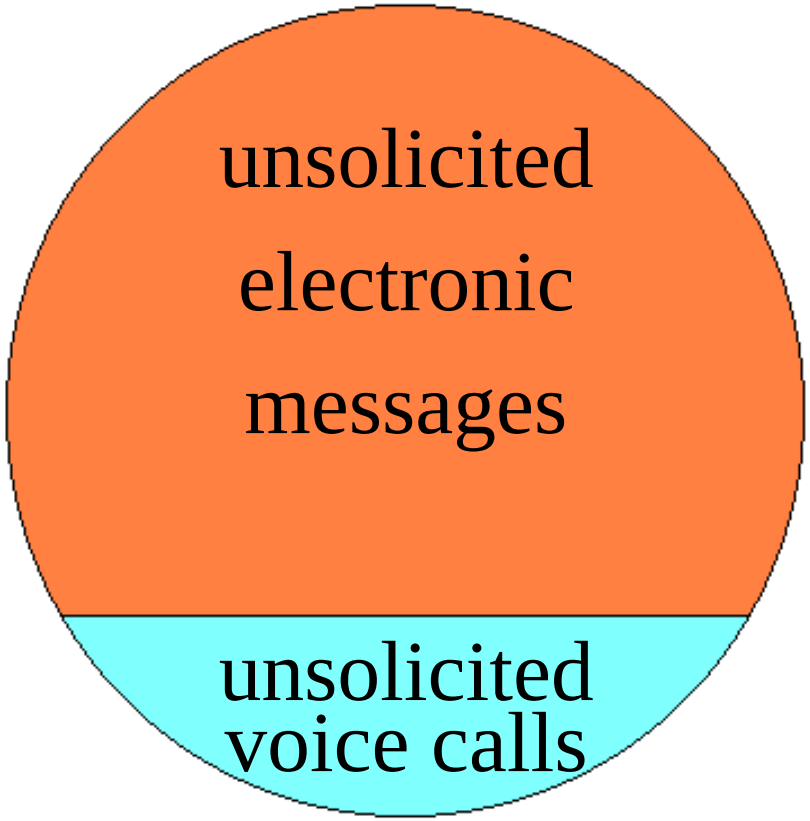
13 January 2004

- Targets
- Prohibitions and safeguards
- Penalties
- Enforcement
- Other measures
- Challenges

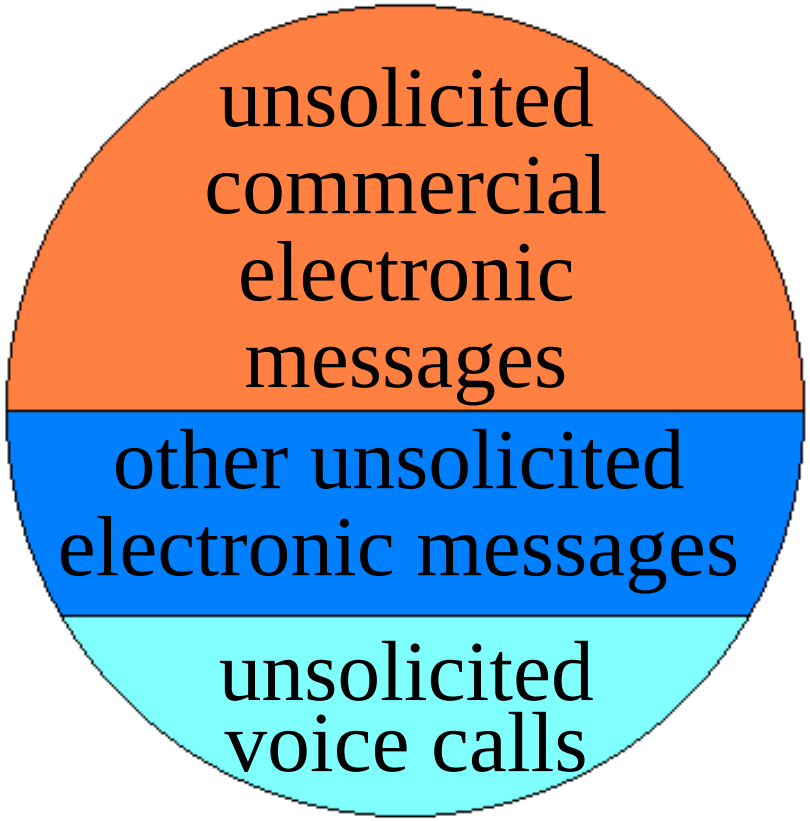
Targets (1)



Targets (2)


unsolicited
electronic
messages
unsolicited
voice calls

Targets (3)


unsolicited commercial electronic messages
other unsolicited electronic messages
unsolicited voice calls

Targets (4)

Unsolicited

	Opt-in	Opt-out
Commercial electronic messages	Australia UK (natural person) US (cell-phone subscribers)	UK (legal person) US (other subscribers)

EU mandates opt-in for natural person but allows member states to choose opt-in or opt-out for legal person

Commercial (1)

- Covers any form of sales promotion, direct marketing by charity and other organizations (e.g.fund raising) - EU
- Includes link to a web page which is ‘commercial in nature’ even if the message itself contains nothing of a ‘commercial nature’ - AUS

Commercial (2)

- Excludes link to the web page of a commercial entity if the message indicates a primary purpose other than commercial advertisement - US

Electronic Message

- Technology neutral - covering SMS, MMS etc
- Excludes voice message left over on a voice mail box - AUS
- Includes voice message left over on a voice mail box. Excludes those for which the simultaneous participation of the sender and the recipient is required - EU

Prohibitions and safeguards (1)

- Sending unsolicited commercial electronic messages
- Sending commercial electronic messages with false or misleading subject line, reply address and information of the sender
- Sending commercial electronic messages unless they include a functional unsubscribe facility

Prohibitions and safeguards (2)

- Supply, acquisition or use of address - harvesting software or a harvested address list or sending randomly addressed (e.g. dictionary attack) mass electronic messages
- Offering of value-added services based on traffic and location data unless subscribers have given their consent and are informed of the data processing implications - UK

Prohibitions and safeguards (3)

- Requirement for anyone who uses cookies (whether they process personal data or not) and similar Internet tracking devices to provide information and offer subscribers a chance to refuse to accept them - UK
- Obligation to give subscribers a right to decide whether or not they want to be listed in subscriber directories - UK

Prohibitions and safeguards (4)

- Accessing a protected computer without authorization and intentionally initiating the transmission of multiple commercial electronic mail messages from or through such computer - US
- Using a protected computer to relay or re-transmit multiple commercial electronic mail messages with the intent to deceive or mislead recipients or ISPs - US

Prohibitions and safeguards (5)

- Sending of commercial electronic mail messages containing sexually oriented material without including in the subject heading the marks or notices prescribed by the commission - US

Penalties (1)

- Monetary penalties or prison terms
- Formal warning, enforceable undertaking, infringement notice, injunction, monetary penalty to recover financial benefits gained and court may order compensation to be paid to a victim. Up to AUS $ 1.1m for a single day. No prison terms - AUS

Penalties (2)

- Monetary penalty, injunction, compensation in many EU member states but criminal sanctions up to terms of imprisonment in some other states
- Up to £ 5,000 in a magistrate court or an unlimited amount if the trial is before a jury. No prison terms. But victim has the right to claim compensation - UK

Penalties (3)

- Up to 90,000 and 3 years in prison - Italy
- Up to US $ 2 m that can be tripled to US $ 6 m for more serious violations and 5 years in prison. Allows ISPs and FTC to sue spammers and state attorneys general to sue on behalf of users - US

Enforcement

- Necessary investigation powers
- Appropriate resources and priorities given to combat spamming
- Complaint and reporting mechanism (rewards not less than 20% of the total civil penalty collected to those supplying information about violation - US)
- Co-operation among authorities

Other measures

- Complementary domestic laws to cover related offences - unauthorized access to computer, protection of personal privacy, deceptive conducts and offensive content
- Users should be aware of their rights, necessary precautions and latest technological tools
- Co-operation of the industry and overseas authorities

Challenges

- Simple and clear targets
- Minimum and necessary prohibitions
- Proportionate and deterring penalties
- Necessary investigation powers and adequate resources for enforcement
- Complementary domestic laws, user and industry involvement as well as international co-operation

Thank you