Privacy Studio.com
The Art of Information Management

THE PRIVACY CASE BOOK:

A Global Survey of Privacy and Security Enforcement Actions with Recommendations for Reducing Risks

CHAPTER 5
Marketing Communications

Margaret P. Eisenhauer, Esq., CIPP
Privacy and Information Management Services – Margaret P. Eisenhauer, P.C.

Chapter Five
MARKETING COMMUNICATIONS

Marketing communications are regulated globally. In the United States, Federal laws broadly regulate telemarketing and all forms of electronic communications (fax, email, and SMS/text messaging). The regulations include preference, content and process requirements. Additionally, these Federal laws generally do not preempt stricter state requirements, and many states have passed legislation regulating marketing communications that impose burdens greater than those required by Federal legislation.[92]

Additionally, while no Federal or state laws generally limit direct mail, some types of direct mail communications are regulated. For example, Federal Trade Commission rules under the Fair Credit Reporting Act mandate an opt-out for pre-screened offers of credit or insurance. Some laws also regulate certain types of communications (such as pharmaceutical product marketing) regardless of medium.

Outside the United States, other countries also regulate marketing communications, including electronic communications and direct mail. Countries with comprehensive data protection laws, such as Australia, Canada, and the European Union member states, require companies to obtain consent for any **secondary use** of personal information.

A **secondary use** is any use of personal information other than as needed to fulfill the purpose for which it was collected. For example, if personal information is collected to process a sales transaction, the use of that information to send a marketing communication is a secondary use.

Given the pervasive nature of marketing, however, and the fact that marketing data is often generated without a primary use (such as when a marketing list is rented), data protection authorities often supplement the general rights provided by their privacy laws with specific legislation or regulation of targeted marketing.

In Canada, for example, the Personal Information and Electronic Documents Act (PIPEDA) imposes a strict preference requirement on the secondary use of personal information for marketing. Companies must offer an opt-out. Per Principle 4.3.3: "An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfill the explicitly specified, and legitimate purposes." This means that you

cannot require individuals to accept your marketing communications; you must instead offer them the ability to opt-out of all such communications.

The Canadian Federal Privacy Commissioner has also published guidance on the use of opt-outs for direct marketing communications. According to her guidance, companies must satisfy the following requirements when using an opt-out regime for secondary marketing purposes:

(1) The personal information must be demonstrably non-sensitive in nature and context.

(2) Information-sharing (if done) must be limited and well-defined as to the nature of the personal information to be used or disclosed and the extent of the intended use or disclosure.

(3) The organization's purposes must be limited and well-defined, and stated in a clear and understandable manner.

(4) As a general rule, organizations should obtain consent for the use or disclosure at the time of collection. In some cases, it may not be reasonably possible to obtain the individual's meaningful consent at the time of collection of the personal information. Principle 4.3.1 recognizes that, in certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before the use or disclosure. In these cases, organizations are encouraged to inform individuals of the proposed use or disclosure, and offer the opportunity to opt out, at the earliest opportunity.

(5) The organization must establish a convenient procedure for opting out of, or withdrawing consent to, secondary purposes. The opt-out should take effect immediately and prior to any use or disclosure of personal information for the proposed new purposes. In cases where there is an existing use or disclosure for secondary purposes, the organization must provide an ongoing mechanism for withdrawing consent to the secondary purpose, and should ensure that the withdrawal takes effect with minimal delay.

Similarly, the European Union member states have all enacted comprehensive data protection laws, generally modeled on the **EU Data Protection Directive (95/46/EC)**.[93] The national laws that implement the Directive all require individuals to be given notice and have choice about whether personal information is used for any secondary purposes, including targeted marketing. This requirement applies to all personal information, including contact information of professionals and commercial customers. Accordingly, at minimum, individuals in Europe have the right to opt-out of any use of their personal data for targeted marketing communications.

The European Union has supplemented the Data Protection Directive with other laws that specifically address certain types of communications. The 1997 Telecommunications Directive[94] was promulgated to address the use of telephonic marketing (phone and fax) by means of automated calling systems and predicative dialers. This directive prohibited the use of these technologies unless express (opt-in) consent of the individuals had been obtained.[95] In 2002, given concerns about the rise of unsolicited commercial email, the European Commission revised, renamed and re-enacted the Telecommunications

Directive as the **e-Privacy Directive**[96] so that it could better address all issues related to electronic communications.

The e-Privacy Directive extends controls on unsolicited direct marketing to all forms of electronic communications including unsolicited commercial email and SMS/text messaging to mobile telephones. It requires prior (opt-in) consent for electronic marketing communications, although countries have established a limited exception for communications within an established customer relationship.

Even countries that do not have established privacy or data protection laws often regulate targeted marketing communications. For example, Mexico regulates marketing communications via the *Ley Federal de Protección al Consumidor* (the Federal Consumer Protection Law). This law was amended in 2000 and again 2003 to expressly provide individuals with the right to opt-out of receiving commercial emails and other unsolicited advertisements (presumably including telephone calls).[97] Laws regulating commercial email (and prohibiting "spam") exist in countries as diverse as Peru, Singapore , New Zealand and China.

General Choice for Marketing Communications

THE BANK STATEMENT STUFFER CASE (JULY 2005)[98]

Respondent: A Bank

Regulator: Office of the Privacy Commissioner of Canada

Basis for Complaint: Violation of Personal Information Protection and Electronic Documents Act Principles 4.3.3 and 4.3.8 regarding choice for secondary marketing.

Facts and Allegations: A bank customer complained to the Privacy Commissioner that his bank continued to include marketing materials in his accounts statements, despite his request to opt-out of receiving direct mail solicitations.

The bank indicated that it had an established suppression program to prevent mailing marketing materials to individuals who had opted out. However, it differentiated the inclusion of statement stuffers ("a generic, non-personalized, non-differentiated, identical message to every customer in the same envelope" as the monthly account statement) to be a use of the consumers' personal information. The bank further viewed "his request to have it manually intercept his monthly credit card statement out of the master production run simply to remove statement stuffers to be unreasonable" especially in light of the fact that some statement stuffers included legally-mandated disclosures to bank customers.

In reviewing the complaint, the Commissioner's Office noted that: "PIPDEA Principle 4.3.3 states that an organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfill the explicitly specified, and legitimate purposes; and Principle 4.3.8 provides that an individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice."

The Privacy Commissioner also considered the concepts of secondary use and disclosure. Although the inserts were not addressed personally to the consumer, "the customer's personal information was still being used, and the goal of placing such inserts was nevertheless one of marketing and was secondary to the reasons for which the complainant initially gave his personal information, namely to receive a credit card."

With regard to choice, the Commissioner also noted that "marketing is marketing," regardless of whether the offers come via phone, direct mail or statement stuffers. She concluded: "the bottom line is that, under the *Personal Information Protection and Electronic Documents Act*, individuals have the right to opt-out of secondary marketing."

The Commissioner's Office consulted with three other major banks regarding their policies on statement inserts. One of the banks did not offer customers the option of opting-out of receiving inserts with their statements. The other two, however, generally allow their clients to opt-out of receiving inserts, depending on the inserts' content. The client can opt-out of receiving inserts about new products, but cannot opt-out of receiving inserts about related services, regulatory information, or information about branch closures. Both banks stated that a very small percentage of clients opt-out of having inserts in their bank statements.

Outcome: The Privacy Commissioner found that the complaint was well-founded, and that the bank's failure to respect the opt-out request violated Principles 4.3.3 and 4.3.8.

The bank agreed to implement a suppression mechanism, so that individuals could opt-out of receiving the statement inserts.

Fine Imposed: None

In Argentina, the National Trade Court also upheld a consumer group's objection to unauthorized marketing. In this case, the Argentine Consumers Union sued Citibank N.A., alleging that Citibank's practice of sharing customer data with marketers unless an opt-out was received violated the country's data protection law.[99] In particular, the complaint alleged that offering an opt-out was not sufficient, that they law required opt-in consent for the data sharing. The Privacy Law Watch reports:

> *The use of clients' information "for a different end, such as its cession to third parties for direct marketing purposes, is alien to the purpose of its collection and requires previous, utter, unequivocal, and informed consent" from the owner of the data, before it can be shared with others, according to the ruling by Judges Martin Arecha, Rodolfo Ramirez, and Angel Sala.*[100]

Similarly, Dr. Omer Tene reports that the Israeli Law and Information Technologies Authority has taken action against companies for inappropriate marketing communications as well.[101] He explains that Israeli bank regulators have recently required banks to divest their holdings in provident funds in an effort to reduce concentration in the financial services industry. These funds have generally been acquired by insurance companies, who wish to send marketing communications to the fund customers for their other products and services. Dr. Tene writes:

> *In December 2007, Israeli Law and Information Technologies Authority ordered insurance companies to cease sending marketing and promotional materials to customers of provident funds under their control, stating such use of customers' data exceeded the original purpose for which the data were collected and is*

therefore prohibited under the Israeli Privacy Protection Act. ILITA held that provision of an opt-out was insufficient as a means to secure customer consent and that customers would have to opt-in in order to legitimize the marketing of insurance products unrelated to pension and retirement savings.

In addition, ILITA rejected the attempt by the insurance companies' parent corporations to register as controllers of provident fund databases, requiring the databases to be registered under the control of provident fund operating companies. Registration of parent corporations as data controllers would arguably permit use of the data by various members of the corporate group, whereas registration of provident fund operating companies as controllers would restrict data use to the provident funds themselves.

Telemarketing

Telemarketing is a method of direct marketing where a seller (or its agent) engages in *"a plan, program, or campaign . . . to induce the purchase of goods or services or a charitable contribution using a telephone."*

In the United States, telemarketing activities are regulated by the Federal Communications Commission and the Federal Trade Commission as well as by the states.

- **The Federal Communications Commission (FCC)** has issued regulations[102] pursuant to the Telephone Consumer Protection Act (TCPA).

- **The Federal Trade Commission (FTC)** has issued its own Telemarketing Sales Rule (TSR)[103] pursuant to the Telemarketing and Consumer Fraud and Abuse Prevention Act.

Both of these regulations have existed since 1991, and both have been amended many times. For example, both the TSR and the TCPA have been amended to accommodate (and regulate) new technology (such as automated/predictive dialers) and to implement the national Do-Not-Call ("DNC") Registry. Both the TSR and the TCPA impose preference, content and process requirements on telephonic communications. They also impose recordkeeping requirements on telemarketers.

The TSR and TCPA are both enforced aggressively by the Federal Trade Commission and Federal Communications Commission respectively. Violations of the TSR and TCPA can result in penalties of up to $11,000 per violation (*i.e.*, each non-compliant call). Additionally, the TSR and TCPA do not generally preempt stricter state regulation of telemarketing. Approximately 43 states have enacted some form of telemarketing regulation. The state attorneys general enforce these laws, and many offer a private right of action as well.

Outside the United States, Canada has enacted national legislation regulating the telemarketing industry and establishing the rights of individuals to opt out of telemarketing. These Telemarketing Rules[104] require companies to (1) maintain internal do-not-call lists that are updated every 30 days, (2)

provide their unique telemarketing registration number upon request, (3) identify the caller, the third party agency and the company in every call, (4) provide a toll-free customer support/service number, (5) refrain from dialing emergency or health care providers, (6) display caller-id information numbers, and (7) refrain from using sequential dialing or automatic dialing and announcing devices.

In Europe, the e-Privacy Directive provides the foundation for national laws regulating telemarketing. Building on the success of the United States Do-Not-Call registry, Australia enacted the Do Not Call Register Act 2006. Under this law, the Australian Communications and Media Authority maintains the no-call registry. Failure to comply with the no-call rules can subject companies to fines of over A$ 1.1 million.

THE DIRECTV, INC. CASE (DECEMBER 2005)[105]

Respondent: DirecTV, Inc.

Regulator: Federal Trade Commission

Basis for Complaint: Violation of the Telemarketing Sales Rule

Facts and Allegations: Respondent is a California-based corporation that sells DirecTV satellite television programming to consumers throughout the U.S. and engages in telemarketing of its services to consumers. DirecTV entered into agreements with five telemarketing companies that made telemarketing calls on behalf of DirecTV.

The FTC complaint alleged that DirecTV violated the Telemarketing Sales Rule (TSR) by:

- Initiating (or causing other companies) to initiate calls to consumers whose numbers are registered with the National Do Not Call Registry;
- Abandoning (or causing other companies) to abandon calls to consumers by failing to connect a live sales representative within two seconds after the end of the consumer's greeting; and
- Providing assistance to at least one telemarketer placing calls on its behalf while knowing or consciously avoiding knowing that the company was violating the TSR.

Outcome: The FTC entered into a consent decree with DirecTV, ordering:

TSR Compliance Program: DirecTV shall develop, implement and maintain a well-documented and easily accessible system to receive and retain telemarketing-related complaints, with each complaint being promptly investigated. The system shall produce detailed monthly reports of telemarketing complaints that include complaints for each authorized telemarketer. For a period of three years after the order, DirecTV shall maintain a procedure of tracking the solicitation of new subscribers, identifying the authorized telemarketer responsible for the sale, and use the information to monitor compliance with the order.

DirecTV shall not violate the TSR directly or through its authorized telemarketers. DirecTV shall not:

(1) Initiate any outbound telephone calls to consumers who requested not to receive calls;

(2) Initiate any outbound telephone calls to a number on the Federal Do Not Call Registry unless it has obtained express agreement in writing, has an established business relationship, or has met the provisions of the TSR Do Not Call safe harbor; or

(3) Abandon calls.

DirecTV is also permanently restrained from:

(1) Failing to conduct reasonable due diligence before making a person an authorized telemarketer;

(2) Failing to obtain a written contract with each authorized telemarketer, including the requirement that it comply with the TSR;

(3) Failing to monitor TSR compliance of authorized telemarketer campaigns and failure to discontinue business when the TSR is violated; and

(4) Providing substantial assistance to a telemarketer when it knows or consciously avoids knowing that the telemarketer is violating the TSR.

Maintenance of Relevant Documents: For a period of six years, DirecTV shall maintain and provide, within 30 days of request, any business records that demonstrate its compliance with this order.

Delivery of Order: For a period of three years after the order, and within five days of service of the order, DirecTV shall deliver a copy of the FTC order to all officers and directors, as well as employees having responsibility relating to telemarketing activities. The order shall be delivered to new employees before assuming responsibilities with DirecTV. In addition, it shall obtain a signed statement from each person acknowledging receipt of the order.

Reporting: For a period of three years, DirecTV shall notify the FTC at least 30 days prior to any corporate change that may affect compliance with the order. Additionally:

(1) Within 30 days of a request by the FTC, DirecTV shall file additional reports, appear for deposition, or provide entry to any business location for FTC inspection;

(2) Within 180 days after service of order DirecTV shall file a report with the FTC setting forth its compliance with the order;

(3) Once every 12 months, after the initial 180 day report, and for three years thereafter, DirecTV shall file a report with the FTC detailing the monitoring activity of its authorized telemarketers;

(4) At the end of each quarter, after the initial 180 day report, and for 3 years thereafter, DirecTV shall file a report with the FTC describing all outbound telemarketing campaigns it conducted or that were conducted by its authorized telemarketers during the previous quarter; and

(5) Upon request of the FTC, DirecTV shall provide more detailed data for telemarketing campaigns.

Fine Imposed: $5,335,000 (When assessed, this was the largest civil money penalty imposed by the FTC in a telemarketing case.)

With the rise of predictive dialers in the late 1990s, consumers became very upset about the number of abandoned and "dead air" calls that they received. The Telemarketing Sales Rule was amended to

address these issues. In particular, the TSR now places strict limits on the call abandonment rates, to help ensure that individuals are not harassed by automated telemarketing systems. The TSR requires companies to connect the consumers called to live operators within 2 seconds of the consumers' completed greetings.

The Federal Trade Commission has opined that the use of pre-recorded marketing messages contravenes the call abandonment provisions because the pre-recorded message is not a live operator. According to the Federal Trade Commission's "Complying with the Telemarketing Sales Rule" guidance (October 2005):

> *Under the Rule's definition, an outbound telephone call is "abandoned" if a person answers it and the telemarketer does not connect the call to a sales representative within two seconds of the person's completed greeting.* ***The use of prerecorded message telemarketing, where a sales pitch begins with or is made entirely by a prerecorded message, violates the TSR because the telemarketer is not connecting the call to a sales representative within two seconds of the person's completed greeting.*** *(emphasis in original)*[106]

The Federal Trade Commission brings enforcement actions against companies that engage in pre-recorded message marketing.

THE BROADCAST TEAM CASE (FEBRUARY 2007)[107]

Respondent: The Broadcast Team, Inc. ("TBT") and various corporate officers

Regulator: Federal Trade Commission

Basis for Complaint: Violation of the Telemarketing Sales Rule (TSR)

Facts and Allegations: Respondent is a Florida-based telemarketer that sells a computerized "voice broadcasting" service that delivers prerecorded messages. This service, "RealCall", uses automated dialers to initiate telephone calls. When a particular call is answered, a computerized system determines whether it has been answered by a live person, an answering machine or voicemail system. The service then delivers prerecorded messages to answering machines, voicemails and/or live people, depending on the particular programming applied. RealCall is capable of placing over one million such telephone calls each day.

The FTC complaint alleged that TBT violated the Telemarketing Sales Rule (TSR) by:

- Abandoning or causing others to abandon calls to consumers by failing to connect a live sales representative within two seconds after the end of the consumer's greeting (over 64 million calls were abandoned since October 1, 2003, when answered by a live person instead of an answering machine or voicemail);
- Initiating calls between October 17, 2003 and January 15, 2004 to consumers whose numbers were registered on the Federal Do Not Call Registry (DNC Registry) and then continuing for several weeks after being instructed by its client to eliminate numbers that were listed on the DNC Registry; and
- Initiating calls on behalf of sellers who (advised by TBT that the fee was not required) had not first paid the required fee to access those numbers on the DNC Registry.

Outcome: The FTC entered into a consent decree with TBT, ordering:

TBT shall not directly violate or cause others to violate the TSR. TBT shall not:

(1) Fail to connect a live sales representative within two seconds after the call is answered by a person and greeting is completed, unless no more than 3% of all calls are abandoned per day, (for calls abandoned under the 3%, a recorded message stating the name and number of the seller must be played within 2 seconds of completed greeting whenever a sales representative is not available);

(2) Initiate any outbound telephone calls to a number on the DNC Registry unless it is made to a business, to solicit charitable contributions, or to a person with whom TzbT has obtained express agreement in writing or has an established business relationship; and

(3) Initiate any outbound telephone calls to numbers within areas without first paying the required annual fee to access the DNC Registry for that area.

Maintenance of Relevant Documents: For a period of five years, TBT shall maintain and provide, within 14 days of request, any business records that demonstrate its compliance with this order.

Delivery of Order: Within 30 days of service of the order, TBT shall deliver a copy of the FTC order to (and obtain signed statements from) all owners, principals, members, officers and directors, as well as employees and all others having decision making authority relating to the subject of the order. In addition, within 10 days of complying, TBT shall provide an affidavit setting forth its compliance with the order.

Reporting: TBT shall notify the FTC at least 30 days prior to any corporate change that may affect compliance with the order. Additionally, for a period of five years, each individual defendant shall notify the FTC within 30 days of any employment or business affiliation changes that involve telemarketing responsibilities.

Fine Imposed: $2,800,000 ($1,000,000 payable within 5 days of order and the remainder suspended)

The Federal Trade Commission continues to make enforcement of the Telemarketing Sales Rule a priority. In November 2007, the Federal Trade Commission announced six settlements with companies alleged to have violated the TSR, including Craftmatic, ADT Security Services and two authorized security system dealers, and Ameriquest Mortgage Company.[108] The settlements collectively imposed nearly $7.7 million in civil penalties.

The announcement also contained information on additional TSR cases that the Federal Trade Commission was filing against Guardian Communications (a company using prerecorded messages, similar to the Broadcast Team) and Global Mortgage Funding.

THE CRAFTMATIC CASE (NOVEMBER 2007)[109]

Respondent: Craftmatic Industries, Inc. and its subsidiaries

Regulator: Federal Trade Commission

Basis for Complaint: Violation of the Telemarketing Sales Rule

Facts and Allegations: Respondent is a Delaware corporation that sells adjustable beds and electronic mobility scooters through its subsidiaries (telemarketers) that call consumers to induce the purchase of its goods and services. Craftmatic ran sweepstakes promotions offering the chance to win a Craftmatic bed after filling out an entry form which indicated the consumers' telephone number was also their entry number. The form did not indicate that by filing it out, they would receive sales calls. Craftmatic, without obtaining the consumers' express consent, then used the information on the entry form to place calls to consumers.

The FTC complaint alleged that Craftmatic violated the Telemarketing Sales Rule (TSR) by:

- Initiating (or causing other companies) to initiate calls to consumers whose numbers are registered with the National Do Not Call Registry;

- Abandoning (or causing other companies) to abandon calls to consumers by failing to connect a sales representative within two seconds after the end of the consumer's greeting; and

- Initiating (or causing other companies) to initiate calls to consumers who previously requested not to receive calls from Craftmatic.

Outcome: The FTC entered into a consent decree with Craftmatic, ordering:

Craftmatic shall not directly violate or cause others to violating the TSR. Craftmatic shall not:

(1) Initiate any outbound telephone calls to consumers who requested not to receive calls;

(2) Initiate any outbound telephone calls to a number on the Federal Do Not Call Registry unless it has obtained express agreement in writing or has an established business relationship; or

(3) Abandon calls by failing to connect a representative within two seconds of a person's greeting unless (a) no more than 3% of all calls are abandoned per day, (b) the phone is allowed to ring for at least fifteen seconds or four rings before disconnecting the unanswered call, (c) a recorded message stating the name and number of the seller is played within two seconds of the completed greeting whenever a sales representative is not available, and (d) records establishing compliance are retained.

Maintenance of Relevant Documents: For a period of five years, Craftmatic shall maintain and provide, within 10 business days of request, any business records that demonstrate its compliance with this order.

Delivery of Order: Within thirty days of the entry of the Order, Craftmatic shall deliver a copy of the FTC Order to all owners, principals, members, officers and directors, as well as managers, agents, servants, employees and attorneys having decision-making authority relating to telemarketing activities. It shall obtain a signed statement from each person acknowledging receipt of the Order. In addition, within ten days of compliance, it shall file an affidavit setting forth its compliance.

Reporting: Craftmatic shall notify the FTC at least 30 days prior to any corporate change that may affect compliance with the order.

Fine Imposed: $4,400,000

As noted above, the Telemarketing Sales Rule and the Telephone Consumer Protection Act rules do not preempt state laws. Most states have laws that regulate telemarketing, and several states have their

own no-call lists. These laws are enforced by state attorneys general or by individuals pursuant to a private right of action.

THE MARKETLINKX CASE (DECEMBER 2007)[110]

Respondent: Marketlinkx Direct, a Florida telemarketer, and its owner, Ezell Brown

Regulator: Missouri Attorney General

Basis for Complaint: Violation of Missouri state telemarketing laws and no-call list requirements

Facts and Allegations: Missouri attorney general sued the respondents after receiving numerous complaints of calls from Marketlinkx to consumers who had registered on the Missouri No-Call list.

Outcome: Marketlinkx and its owner entered into a voluntary assurance pursuant to which they agreed to cease calling Missourians on the No-Call list and otherwise comply with Missouri laws.

In addition to a fine, Respondents agreed to pay future civil penalties of up to $2,000 for violations of the assurance agreement and a $5,000 per violation penalty for any violations of state consumer protection laws.

Fine Imposed: $15,000

State telemarketing law enforcement is a priority for Missouri Attorney General, Jay Nixon, and many of his counterparts in other states. In Missouri, for example, over 2.5 million people have registered on the state No-Call Registry.[111] According to a story in the *Branson Daily News*, the Marketlinkx action brings the total collected from No-Call violators to $1,713,500 since July 2001.[112] The story notes that in July 2007, Mr. Nixon's office fined a Florida mortgage broker $155,000 and a satellite TV marketing company $330,000.

Concerns about unsolicited calls and mobile phone marketing have prompted international regulators to take action against companies as well. Regulators in countries with established privacy laws frequently bring actions when companies fail to respect opt-out requests.

THE IDD PROMOTION CASE (JANUARY 2007)[113]

Respondent: Telecommunication Company promoting an IDD service

Regulator: Privacy Commissioner for Personal Data ("PCPD")

Basis for Complaint: Violation of Section 34(ii) of the Hong Kong Personal Data (Privacy) Ordinance

Facts and Allegations: A consumer complained to the PCPD about telemarketing calls promoting an international direct dialing (IDD) service. The consumer indicated that, despite his requests not to be called, the telecommunications company had called him on four occasions.

The PCPD determined that the calls contravened Section 34(ii) of the Ordinance and referred the matter to the police for prosecution.

Outcome: The telecommunications company pleaded guilty to five counts of violating Section 34 (ii).

Fine Imposed: HK$14,000, representing HK$5,000 for the first violation and HK$ 3,000 for each subsequent violation

Even regulators in countries without developed privacy laws have found ways to take action against companies that flaunt consumer privacy interests in their cell phones.

THE AIRTEL CASE (JULY 2007)[114]

Respondents: Airtel, the Cellular Operators Association of India and financial firms ICICI Bank and American Express

Regulator: This case involves a complaint filed by a consumer group with the Delhi State Consumer Disputes Redressal Commission (an Indian consumer court)

Basis for Complaint: Violations of Privacy, Nuisance

Facts and Allegations: A consumer complaint alleged that the respondents made unwanted telemarketing calls and sent unsolicited text messages to mobile phone users, amounting to harassment and an invasion of privacy. The complaint also alleged that recipients of the marketing messages had to bear the costs of the messages via roaming charges.

Outcome: The court concluded that the calls and messages were a "nuisance and disturbance" and they violated the consumers' rights of privacy. The judge noted that fines were appropriate because the respondents knew they were placing a burden on consumers when they made the calls.

Fine Imposed: 7.5 million Rupees (approximately $170, 500)

Fax communications

The delivery of unsolicited marketing communications via facsimile is regulated under United States and international laws. Because fax transmissions are considered intrusive (often causing consumer phones to ring at night) and because recipients incur real costs in receiving faxes (such as costs associated with paper and machine cartridges), fax rules are generally well enforced.

In the United States, faxes are regulated by the Federal Communications Commission, under the Telephone Consumer Protection Act or TCPA (discussed above). The Federal Communications Commission enforces these rules. Several states also regulate fax communications under their own state telemarketing regimes. Because the TCPA does not preempt stronger state laws, the state fax rules often exceed the Federal Communications Commission's rules. For example, California law

generally requires senders to have opt-in consent to transmit marketing faxes.[115] Approximately fifteen other states have similar opt-in rules for faxes.

In Canada, the telemarketing rules discussed above also regulate unsolicited commercial faxes. Canadian law requires opt-out consent for commercial faxes and imposes similar content regulations as with telemarketing.

THE FAX.COM, INC. CASE (AUGUST 2002)[116]

Respondent: Fax.com, Inc.

Regulator: Federal Communications Commission

Basis for Complaint: Violation of the Telephone Consumer Protection Act (TCPA)

Facts and Allegations: Respondent is a California-based corporation that operates as a "fax broadcaster", sending messages to telephone facsimile machines on behalf of other entities for a fee. These messages advertise either the commercial availability or quality of a product, good or service and therefore constitute advertisements. Fax.com sent its clients' advertisements using its own distribution list of facsimile numbers without verifying that the recipient had 1) consented to receive the fax or 2) had an established business relationship with Fax.com or its client. In addition, Fax.com did not disclose to its clients the prohibition regarding faxing unsolicited advertisements. The FCC issued citations in December 2000 and May 2001 informing Fax.com of its violations of the TCPA and that it could be subject to monetary forfeitures if it continues sending unsolicited facsimile advertisements.

The FCC Notice of Apparent Liability for Forfeiture alleged that Fax.com violated the Telephone Consumer Protection Act by:

- Sending unsolicited advertisements to telephone facsimile machines on 489 separate occasions;
- Not having an established business relationship with the consumer; and
- Not having prior written consent from the consumer for the faxes to be sent.

Outcome: By Order of Forfeiture to Fax.com, the FCC ordered Fax.com to come into compliance with the TCPA and the FCC's rules and orders. It further ordered:

Reporting: Fax.com shall file a report with the FCC within 30 days of the Order indicating whether it has come into compliance with the TCPA and FCC rules prohibiting unsolicited advertisements to telephone facsimiles.

Fine Imposed: $5,379,000

In Europe, fax transmissions are regulated generally by data protection laws and specifically by national laws that implement the Privacy and Electronic Communications Directive (the "e-Privacy Directive").[117]

THE UK FAX CASES (2007)[118]

Respondent: Case 1: ADC Organisation Limited (July 2007)
Case 2: Clear Debt Solutions Limited (September 2007)

Regulator: Information Commissioner (UK)

Basis for Complaints: Violation of the Privacy and Electronic Communication (EC Directive) Regulations 2003 (the "Regulations")

Facts and Allegations: Respondents are UK-based companies that engage in fax marketing.

The regulations require that marketing faxes may only be sent to recipients who are (a) individuals who have opted-in to receiving the faxes, or (b) corporate subscribers who have not opted out. Additionally, no faxes may be sent to numbers registered with the Fax Preference Service. The complaints alleged that respondents sent marketing faxes in violation of Regulations.

Outcome: By Order of the Information Commissioner, respondents must, within 30 days, cease all violations of the Regulations.

Fine Imposed: None

Email Communications

Concerns around unsolicited commercial email and spam have prompted many countries to enact laws regulating the transmission of unsolicited commercial email messages. These laws are generally well enforced globally.

In the United States, the **Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM)** regulates the transmission of commercial electronic mail messages. A commercial electronic message is any email whose primary purpose is the advertisement or promotion of a commercial product, service or website.[119] The CAN SPAM Act is being implemented through regulations promulgated by the Federal Trade Commission and the Federal Communications Commission.

The CAN-SPAM Act imposes preference, content and process requirements on senders of commercial emails. The Federal Trade Commission, Federal Communications Commission, state attorneys general and Internet service providers bring actions to address CAN-SPAM Act violations.

THE MEMBER SOURCE MEDIA CASE (JANUARY 2008)[120]

Respondent: Member Source Media LLC

Regulator: Federal Trade Commission

Basis for Complaint: Violation of the CAN SPAM Act; deceptive trade practices in violation of Section 5 of the FTC Act (see Chapter 2)

Facts and Allegations: Member Source operates the ConsumerGain.com, PremiumPerks.com, FreeRetailRewards.com, and GeatAmericanGiveaways.com, websites. Member Source used emails to attract consumers to these websites.

The FTC alleged that the Member Source emails were deceptive, in violation of the CAN SPAM Act and Section 5 of the FTC Act. For example, Member Source sent emails to consumers with subject lines such as "Congratulations. You've won an iPod Video Player"; "Here are 2 free iPod Nanos for You: confirm now"; "Nascar Tickets Package Winner"; "Confirmation required for your $500 Visa Gift Card"; or "Second Attempt: Target Gift Card Inside." Consumers that came to the websites saw similar statements, such as "CONGRATULATIONS! You Have Been Chosen To Receive a FREE GATEWAY LAPTOP." However, when consumers arrived at the Member Source websites, they were led through a series of ads for goods and services from third parties. To "qualify" for their "free products," consumers had to view pages of third party offers and "participate in" third party promotions by purchasing products, subscribing to satellite television service, or applying for credit cards.

The FTC alleged that, because consumers had to pay money and otherwise provide consideration to get the "free gifts" the subject lines in the Member Source emails were deceptive, in violation of the CAN SPAM Act. Additionally, because Member Source failed to disclose material facts, such as the fact that the consumers had to pay to obtain the "free products", its actions were deceptive in violation of the FTC Act.

Outcome: Member Source Media is permanently restrained and enjoined from:

(1) In any email and online advertisement, and on any landing page associated with such email or online advertisement, that contains any direct or implied representation made by Defendants, or made by any authorized agent on behalf of Defendants, that a product or service is free, failing to disclose, in the same color, font, and size, and within close proximity to such representation that a purchase is required, or that purchases are required, to obtain such product or service, when such is the case;

(2) On any landing page associated with any direct or implied representation made by Defendants, or made by any authorized agent on behalf of Defendants, that a product or service is free, failing to disclose, in a clear and conspicuous manner: (a) a list of the monetary obligations a consumer is likely to incur to obtain the advertised product or service, when such is the case; (b) a list of any non-monetary obligations a consumer is likely to incur to obtain the advertised product or service, such as having to apply and qualify for credit cards or an automobile loan, when such is the case. (These disclosures may be made from such landing page via a hyperlink, provided that the hyperlink is labeled to convey the nature and relevance of the information to which it leads, and is clearly and conspicuously disclosed.); and

(3) Violating the CAN-SPAM Act including, but not limited to, by initiating the transmission of a commercial email message that misrepresents the content or subject matter of the message.

Record Keeping: For a period of eight (8) years, Member Source must create and retain:

(1) Accounting records that reflect the cost of goods or services sold, revenues generated, and the disbursement of such revenues;

(2) Personnel records accurately reflecting: the name, address, and telephone number of each person employed in any capacity by such business, including as an independent contractor; that person's job title or position; the date upon which the person commenced work; and the date and reason for the person's termination, if applicable;

(3) Customer files containing the names, addresses, phone numbers, dollar amounts paid, quantity of items or services purchased, and description of items or services purchased, to the extent such information is obtained in the ordinary course of business;

(4) Complaints and refund requests (whether received directly, indirectly or through any third party) and any responses to those complaints or requests; and E. Copies of all sales scripts, training materials, advertisements, or other marketing materials;

(5) Records demonstrating reasonable policies and procedures to process and handle customer inquiries and complaints; and

(6) All records and documents necessary to demonstrate full compliance with each provision of this Order.

Fine Imposed: $200,000

As noted above, Australia has a comprehensive data protection law, which includes the general types of fair information practices provisions that have been discussed already. The Australian National Privacy Principles specifically address the use of personal information for secondary uses including marketing.

Additionally, Australia has implemented the Spam Act 2003 which regulated electronic marketing including email and text messages. In March 2005 the Australian Communications and Authority (ACMA), the regulatory body charged with enforcing the Spam Act, issued the Australian e-Marketing Code of Practice Guidelines.[121] The Australian rules regarding commercial email are very well enforced.

THE AUSTRALIAN SPAM CASES (JULY 2007)[122]

Respondent: Case 1: DC Marketing Europe Ltd. (a company incorporated in the UK, with a registered office in Sydney, Australia)

Case 2: Pitch Entertainment Group (Pitch)

Case 3: Clarity1 Pty Ltd (Clarity1) and company managing director, Mr. Wayne Mansfield

Regulator: Australian Communications and Media Authority (ACMA)

Basis for Complaint: Violations of the Spam Act 2003 (Australia)

Facts and Allegations: Case 1: DC Marketing engaged in "missed call" marketing programs in Australia. In particular, the company would place short calls to cell phones, resulting in "missed call" messages appearing on the phones. When individuals returned the calls, they received pre-recorded marketing messages. ACMA alleged that the marketing calls violated the Spam Act because they were unsolicited communications that did not appropriately identify the sender or offer an opt-out.

Case 2: ACMA alleged that Pitch sent over one million commercial electronic messages to mobile phones without a functional unsubscribe facility.

Case 3: ACMA alleged that Clarity1 and Mr. Mansfield sent out at least 231 million commercial emails that were unsolicited and otherwise in breach of the Act.

ACMA alleged that the marketing calls violated the Spam Act because they were unsolicited communications that did not appropriately identify the sender or offer an opt-out.

Outcome: Cases 1-2: ACMA resolved the matters internally and imposed fines as provided for by the Act. ACMA also entered into formal undertakings with the respondents regarding ongoing compliance with the Act, including: (a) sending messages with only recipients' consent; (b) including accurate information about the sender in the message, and (c) offering a functional unsubscribe option in the message.

For example, in its undertaking with ACMA, Pitch agreed to ensure that:

- All future messages contain a functional unsubscribe facility;
- It is capable of receiving unsubscribe requests;
- Its staff receive training in the Spam Act and are informed of the undertaking;
- Its systems and processes comply with the Spam Act; and
- It will audit its messages and report to ACMA on the number of messages sent with an unsubscribe facility, the number of unsubscribe requests received and the steps it has taken to act on unsubscribe requests.

Case 3: ACMA referred the case to Federal Court for prosecution.

Fines Imposed: Case 1: A$ 149,600 (approximately $132,000) for 102 violations of the Spam Act

Case 2: A$11,000

Case 3: Federal Court ordered penalties of A$.5 million against Clarity1and A$1 million against Mr. Mansfield

In Argentina, the very first action brought under the country's data protection law was a spam case. According to a BNA Privacy Law Watch article, two Argentine lawyers sued Carlos Cosa, an individual who had repeatedly sent them unsolicited commercial email and refused to honor opt-out requests. The lawyers claimed that Cosa's actions violated the Argentine Personal Data Protection Act. The court found for the lawyers and enjoined Cosa from sending any further emails to the lawyers.[123]