



International Distribution Institute

Disputes Over Customers' Data

Obtaining Post-Termination Protection:
The U.S. Litigation Perspective

Unauthorized 3rd-Party Access



- Hacking of software provided by hotel franchisor to franchisees to access customer data
- Led to FTC enforcement action against franchisor
FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015)
- Followed by private class action customer, shareholder litigation

Protectable Customer Data



- Information obtained **from** the customer
- Information provided **to** the customer
- Information **about** the customer, including:
 - identity of the customer
 - the customer's needs and history (e.g., product purchases, usage, repair)

Sources of Legal Protection

- Breach of contract (*e.g.*, license, dealer, distribution, franchise agreement, NDA)
 - What if the contract is silent or ambiguous about who owns or can use the data?
- Misappropriation of trade secrets
 - What if confidentiality was not adequately maintained or has since been lost?
- Federal and state computer crimes laws

What about copyright law?



- U.S. protects only original works of authorship
- Sweat of the brow doctrine
 - Rights obtained by diligence (e.g., database or directory)
 - Substantial creativity or "originality" not required
 - U.S. Supreme Court rejected *Feist Publ'ns v. Rural Tel. Serv.*, 499 U.S. 340 (1991)
 - Compilations protected only if originality or creativity in selection
17 U.S.C. § 101

Remedies for wrongful access

- Preliminary injunctive relief
 - What if it is too late to maintain confidentiality?
- Compensatory or punitive damages
- Unjust enrichment and disgorgement
- Recovery of costs and attorneys' fees
 - Only if authorized by contract or statute
- Sealing the court record
 - Generally disfavored but may be appropriate



Remedies for wrongful access

Potential Cause of Action	Preliminary injunction	Damages	Costs and attys' fees	Other remedies
Uniform Trade Secrets Act	✓	✓	✓	
Defend Trade Secrets Act	✓	✓	✓	Ex parte seizure order
State Computer Crimes Laws	✓	✓	✓	Sealing the record
Computer Fraud & Abuse Act	✓	✓	✓	
Electronic Commc'ns Privacy Act	✓	✓	✓	

Preliminary injunctive relief



- Likely the only effective remedy if no use or disclosure yet
 - Prohibitory injunction
 - Mandatory injunction requiring return or destruction, assignment of patents and other IP
Ex parte seizure orders
- But what if disclosure has already occurred?

Trade secrets on the Internet



- Early view
 - “Once a trade secret is posted on the Internet, it is effectively part of the public domain, impossible to retrieve.”

Religious Tech. Ctr. v. Lerma, 908 F. Supp. 1362, 1368 (E.D. Va. 1995);
Religious Tech. Ctr. v. Netcom, 923 F. Supp. 1231 (N.D. Cal. 1995)
(denying preliminary injunction to retrieve Church of Scientology trade secrets disclosed by former parishioners and clergy)

Trade secrets on the Internet



- Later view
 - Not lost if posting “sufficiently obscure or transient or otherwise limited so that it does not become generally known to ... potential competitors”

DVD Copy Control Ass'n v. Bunner,
10 Cal. Rptr. 3d 185 (Ct. App. 2004)

Trade secrets on the Internet



- Key factors
 - How long was it posted?
 - How promptly did the owner act to retrieve the posting?
 - Who saw it in the interim?
 - How accessible and popular are the site?
 - Where does it show up in search engine queries?
 - How much was disclosed?

Preliminary injunctive relief

- Intended to preserve “status quo,” *i.e.*, “last, actual peaceable uncontested status”
- If information is already on the Internet, is the “status quo” that it is no longer a trade secret?
- Computer crimes laws require no showing of trade secret protection
- Arbitration clause
 - What if no carve-out for preliminary injunctive relief, *e.g.*, to protect IP?
 - Authority that federal courts have inherent power to preserve status quo pending arbitration
 - Is it still good law now that ADR rules authorize preliminary injunctions?

U.S. trade secret law

- State law
 - Common law tort of trade secret misappropriation
 - Uniform Trade Secrets Act enacted in 48 states (all but New York & North Carolina) + the District of Columbia, Puerto Rico, Virgin Islands
- Federal law
 - Defend Trade Secrets Act added civil remedies to Economic Espionage Act
- Trade secrets
 - Independent economic value from **not** being generally known to and **not** being readily ascertainable by proper means by others
 - Efforts “reasonable under the circumstances” to maintain secrecy
- Misappropriation
 - Disclosure or use of data obtained wrongfully

Trade secrets in franchising



- Strategic information
- Computer software
- Customer information
- Recipes and formulas
- Methods of operation
- Operations manuals
- Prospective franchisees
- Product line extensions
- Supply agreements

State computer crimes laws



- Prohibit “use” of computers “without authority”
- Some allow civil remedies
 - Sealing the record
 - Injunctive relief
 - Costs and attorneys’ fees
- Criminal statute may also support common law claim (“trespass to chattels”)

State computer crimes laws

- Hacker reconstructed and sold customer list
 - *Ex parte* orders sealing record, granting TRO and preliminary injunction
UPS, Inc. v. Matuszek, Case No. 1:97-cv-00744 (E.D. Va. 1997)
- Failure to disclose disabling code violated state and federal law
Roller Bearing Co. of America, Inc. v. American Software, Inc., Case No. 3:07-cv-01516 (D. Conn.)
- Terminated dealer continued to access “dealers only” portal
 - Ordered to pay attorneys’ fees and cost of having forensic expert image and analyze computers in Tennessee, Arkansas, Alabama, and Mississippi
NACCO Materials Handling Group, Inc. v. The Lilly Co., 278 F.R.D. 395 (W.D. Tenn. 2011)

Federal computer crimes laws



- Electronic Communications Privacy Act (ECPA)
 - Wiretap Act prohibits unauthorized interception of communications
 - Stored Communications Act prohibits unauthorized dissemination or review
- Computer Fraud & Abuse Act (CFAA)

Computer Fraud & Abuse Act

- Prohibits intentional access to computer without authorization or exceeding authority
 - Recent decisions hold that employee access for an unauthorized purpose is **not** “without authorization”

Van Buren v. United States, 593 U.S. ___ (2021); *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012); *U.S. v. Nosal*, 676 F.3d 854 (9th Cir. 2012)
- Damages if > \$5,000
 - “any reasonable cost to any victim”
 - “cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense”
 - Some courts require “interruption of service” for an award of damages

Follow-up

Q&A



Contact

Michael J. Lockerby

Partner

FOLEY & LARDNER LLP

Washington Harbour

3000 K Street, N.W., 6th Floor

Direct dial: 202.945.6079

Mobile: 804.399.6089

Email: mlockerby@foley.com

www.foley.com



International Distribution Institute

Disputes over customers' data

The Dutch Perspective

IDI Conference 2024
14 -15 June 2024
Prague

Who owns customers' data ?

Commercial agency relationships

- It is not clear in a commercial agency relationship who owns the customer data; it will depend on what the parties have agreed.
 - In a recent court case, the Dutch court decided it does not read into the statutory definition of an agency agreement that the commercial agent is obliged to give all customer data to the principal. Nor does the court read into the legal definition that the customers of the principal are always (exclusively) involved. The commercial agent acts as an intermediary in the formation of agreements, but it does not follow from this that it exclusively concerns customers of the principal (*ECLI:NL:RBNHO:2023:3528*)
 - Upon termination of the relationship the principal may have to pay the agent a goodwill compensation. Furthermore the parties may have agreed on a non-compete, effectively preventing the agent from using the customer data for a certain period of time.

Who owns customers' data ?

Franchise relationships

- Also in franchise relationships, the Dutch Franchise Act does not clarify who owns the customers' data.
- However the Dutch Franchise Act does state that when the franchisor takes over the franchise operation from the franchisee, the franchisor is obliged to pay the franchisee a goodwill compensation. This implies that the customer base will then also be transferred to the franchisor. However there is no case law yet on this topic.
- Loyalty cards: depending who operates the loyalty card, the customer data may be owned by respectively the franchisor or the franchisee.

Who owns customers' data ?

Franchise relationships

- Mandatory transfer of client portfolio valid?
 - The Amsterdam Court of Appeal ruled that a compulsory transfer of customers at the end of a franchise agreement is not unacceptable by the standards of reasonableness and fairness as there is compensation in return and franchisee is otherwise not hampered in his livelihood (ECLI:NL:GHAMS:2017:4229)

Who owns customers' data ?

Distribution / dealer relationships:

- After termination of the distribution agreement, it depends on the circumstances and on what the parties have agreed, who owns the customer data. There is no automatic transfer of customer data to supplier, so without a contractual provision, supplier has no right to exploit such database.
- However the distributor has to act careful ('*zorgvuldig*') towards its former supplier:
 - Considering the number of clients distributor approached, the fact that distributor only knew these clients through his distributorship for supplier and the purport of the message he sent them, the distributor, in the opinion of the court in preliminary relief proceedings, exceeded the standard of care referred to here by systematically approaching suppliers' clients, using the information he had obtained under the distribution agreement. In doing so, distributor acted unlawfully towards supplier and is liable for the damage supplier suffered as a result. (*ECLI:NL:RBZLY:2008:BG8690*)

Who owns customers' data ?

Intellectual property rights:

The following intellectual property rights may play a role and may also protect as party against the use of customer data by the other party:

- Database rights
- Copyrights
- Trade secrets

Who owns customers' data ?

Unfair competition

The use of customer data by a party may qualify as unlawful competition, under the following circumstances, if the following cumulative requirements are met:

- 1) the systematic and substantial erosion.
- 2) of the former contract party's sustainable market share, which the other party helped to build during their cooperation and
- 3) with the resources - such as knowledge, experience and data - that the party received confidentially from his former contract party for this purpose.

The court must fill in these requirements based on the circumstances of the case.

This is not based on an act, but developed consistently in case law and confirmed by the Dutch Supreme Court.

Use of contractual clauses on customers' data



Allows to consider the way in which customer's data will be used at different stages of the contractual relationship:

- Performance
- After termination

Contractual clauses can in exceptional circumstances be declared unenforceable, where considered to be **unacceptable** according to the standard of **reasonableness and fairness**



Impact of personal data regulation

- Complying with the personal data regulation helps to clarify the various uses of personal data, parties involved in the processing of data, purposes of every data processing.
- It also allows to identify who is the “controller” in the meaning of the GDPR, which helps to determine who owns customers’ data.
- The “controller” determines the purposes and essential means of the processing. Essential means refer notably to :
 - Type of personal data
 - Types of data subjects
 - Duration of processing
 - The recipients



International Distribution Institute

Disputes over customers' data

The French Perspective

IDI Conference 2024
14 -15 June 2024
Prague

Jean-Philippe ARROYO
J.P. Karsenty & Associés
jpharroyo@jpkarsenty.com

Who owns customers' data ?

Agency

- The customer base belongs to the principal, not to the agent :
 - The agent exploits the customer base of the principal, whose products it distributes. Therefore, the use of its own customer base excludes the status of commercial agent (*Court of cassation, 10 July 2007, n° 05-19.373*)
 - « The commercial agent, as a mere representative, has no customers of his own » (*Court of cassation, 29 June 2010, n° 09-66.773*)

Who owns customers' data ?

Franchise

- The question of ownership of customers' data takes on several aspects:
 - Local customers : The local customer base belongs to the franchisee who implements the necessary means to attract local customers and bears the risks of the business. (*Court of cassation, 27 March 2002, n° 00-20,732*)
 - National customers : At national level, the customer base is attached to the reputation of the franchisor's brand (*Court of cassation, 27 March 2002, n° 00-20,732*)
 - Loyalty cards : The customers' database arising from the loyalty cards implemented by the franchisor, belongs to the franchisor who supports the funding of such loyalty program. For the Court, the loyalty customer base is considered to be attached to the shop brand, not to the physical shop in itself. (*Chambery Appeal Court, 2 October 2007, n° 06/01561*)

Who owns customers' data ?

Distribution agreement :

- After termination of the distribution agreement, the dealer retains its local customer base, independent from the licensed brand (*Court of cassation, 26 June 2007, n° 06-12.077*)
- When the distributor has constituted its customers' database and absent any contractual clause, the supplier has no right to exploit such database after termination of the contract. The distributor has therefore its own customers' base. (*Paris Court of appeal, 30 October 2019, n° 17/14440*)
- The customer base constituted by the dealer for the exploitation of the supplier's car brand is attached to the brand and therefore allows the supplier to exploit the customers' database after termination of the distribution agreement (*Court of cassation, 6 May 2008, 06-11.968*)

Use of contractual clauses on customers' data



Allows to consider the way in which customer's data will be used at different stages of the contractual relationship:

- Performance
- After termination

Contractual clauses can sometimes be declared unenforceable, where considered to create a **significant imbalance** between the parties

Use of contractual clauses on customers' data

Case law in a franchise context

Existence of a clause

- Where the clause stipulates that the franchisee has the exclusive ownership of the customers' database, the franchisor cannot exploit such database after termination of the contract (*Paris Court of Appeal, 14 January 2002, Audika*)
- A clause of the franchise agreement provided that the franchisor was allowed to modify or replace the operating software. After deciding to replace the operating software, the franchisor concluded a licence agreement with its provider and asked its franchisees to sign the sub-licence agreement. The appendix of the sub-licence agreement allowed the franchisor to activate or deactivate the franchisees sub-licences, depriving them of all access to their customers' data. The Court held that, regarding the substantial change in the terms and conditions of the franchise agreement created by such a clause, the franchisees' termination was fully justified. (*Paris Court of appeal, 10 May 2017, n° 14/201469*)

Use of contractual clauses on customers' data

- Case law in a franchise context

Existence of a clause – the notion of significant imbalance

- The Paris Court of appeal considered that the franchise agreement's clause which provided that the franchisor was entitled to save the franchisee's customers' database after termination of the contractual relationship, without payment of any compensation, was constitutive of a substantial breach of the economy of the contract and constituted a manifest imbalance between the parties' respective obligations (*Paris Court of appeal, 29 April 2014, n° 13/04683*)

Use of contractual clauses on customers' data

-

Case law in a franchise context

Absence of a clause

- In general, absent a clause, the Courts have a general trend to protect the franchisee's database
 - The Court of cassation approved the Court of appeal decision which upheld an interim order prohibiting the franchisor from using the franchisee's customers' database. Indeed, the franchisor used customers' database to promote the opening of a new shop under the franchisor's sign and refused to transfer the customers' database to the franchisees, even though no clause allowed the franchisor to access such database after termination of the contract (*Court of cassation, 27 September 2023, n° 22-19.436*)

- Nevertheless, the franchisor is sometimes recognised as being entitled to exploit the customer database
 - The fact that the franchisee has developed its own customer base locally does not mean the franchisor has not developed a national customer base attached to the brand reputation. Therefore, as the customers' database was set up and operated by the franchisor, who moreover never undertook not to use it towards the franchisee's clients after termination, the franchisor is allowed to exploit the customers' database to inform customers of the opening of a new shop under the franchisor's brand. (*Rennes Court of appeal, 28 June 2011, n° 10/00903*)

Unfair competition

Agency

After termination of the agency contract, the sending, by the former agent, of a letter to the customer base of its former principal must be regarded as unfair competition (*Court of cassation, 19 July 1965*)

Franchise

In presence of a contractual clause providing that the customer's database is the exclusive ownership of the franchisee, it is impossible for the franchisor, after the contract's termination to use the database for its own benefits. Such behaviour constitutes unfair competition (*Paris Court of Appeal, 14 January 2002*)

Distribution agreement

"The use by the supplier of the customer's database of its former dealer, at the end of the exclusive distribution contract, constitutes an act of unfair competition" (*Court of cassation, 16 February 2022, n° 20-22.572*)

Impact of personal data regulation

- Complying with the personal data regulation helps to clarify the various uses of personal data, parties involved in the processing of data, purposes of every data processing.
- It also allows to identify who is the “controller” in the meaning of the GDPR, which helps to determine who owns customers’ data.
- The “controller” determines the purposes and essential means of the processing. Essential means refer notably to :
 - Type of personal data
 - Types of data subjects
 - Duration of processing
 - The recipients