M E M O R A N D U M

Jan. 17, 2017 revised Feb. 19, 2017

From: Stephen Y. Chow

To: ULC Drafting Committee on the Unauthorized Disclosure of Intimate Images Act

Re: Uniform Trade Secrets Act Misappropriation as Template for Information Privacy

With the rise of interest and value in personal information and its misuse in the "cloud," I suggest looking to the template of "misappropriation" of the Uniform Trade Secrets Act ("UTSA"), one of the Conference's most successful products (47 States, DC, similar North Carolina law and New York following the *Restatement (Third) of Unfair Competition* that endorses UTSA). Congress enacted 87-0 and 410-2 the Defend Trade Secrets Act of 2016 ("DTSA"), which adopts the UTSA definition of "misappropriation" and applies it to a federal private right of action for misappropriation of 1996 Economic Espionage Act ("EEA") "trade secrets."

Personal information privacy has received limited protection in the United States under federal sectoral laws, such as the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act, and under state common law (sometimes codified) of protection against outrageous "intrusion" as stated by Justice Brandeis and by Dean Prosser in the Restatement (Second) of Torts. Privacy commentators have lamented the limitation of personal privacy to the four Brandeis/Prosser torts of "intrusion"-type breach of privacy, and some have suggested following the alternative UK law, which had "forked" in the 1980s to a theory of breach of confidence to protect personal information privacy.[1]

UTSA (and now DTSA) "misappropriation" addresses both "improper" intrusion and breach of confidence types of breach of information privacy.

Thus, the UTSA may provide a template for the States to develop personal information privacy law based on both branches. Following is a possibility of replacement of "*private information*" for "trade secrets"[2] in the bracketed language:

"Misappropriation" means:

> (i) acquisition of [a trade secret] [*private information*] of another by a person who knows or has reason to know that the [trade secret] [*private information*] was acquired by improper means; or

[1] *E.g.*, Richards & Solove, PRIVACY'S OTHER PATH: RECOVERING THE LAW OF CONFIDENTIALITY, 96 GEO. L.J. 124 (2007); GILES, PROMISES BETRAYED: BREACH OF CONFIDENCE AS A REMEDY FOR INVASIONS OF PRIVACY, 43 BUFFALO L. REV. 1 (1995); Vickery, BREACH OF CONFIDENCE: AN EMERGING TORT, 82 COLUM. L. REV. 1486 (1982); *see also* Scholz, PRIVACY AS QUASI-PROPERTY, 101 IOWA L. REV. 1113 (2016) (trade secrets and information privacy as quasi-property, *i.e.*, dependent on a relationship rather than purely against public); Hartzog, REVIVING IMPLIED CONFIDENTIALITY, 89 IND. L.J. 763 (2014).

[2] In the Nineteenth Century jurisprudence recognizing protection of a "secret of trade," a "secret of title" was also recognized, *e.g.*, Peabody v. Norfolk, 98 Mass. 452, 459 (1868), the latter protected today in financial privacy.

(ii) disclosure or use of [a trade secret] [*private information*] of another without express or implied consent by a person who

(A) used improper means to acquire knowledge of the [trade secret] [*private information*]; or

(B) at the time of disclosure or use, knew or had reason to know that his knowledge of the [trade secret] [*private information*] was

(I) derived from or through a person who had utilized improper means to acquire it;

(II) acquired under circumstances giving rise to a duty to maintain its [secrecy] [*privacy*] or limit its use; or

(III) derived from or through a person who owed a duty to the person seeking relief to maintain its [secrecy] [*privacy*] or limit its use; or

(C) before a material change of his position, knew or had reason to know that it was [a trade secret] [*private information*] and that knowledge of it had been acquired by accident or mistake.[3]

"Improper means" includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain [secrecy] [*privacy*], or espionage through electronic or other means;[4]

A possible definition of "private information" may also be based on the UTSA template:

["Trade secret"] [*"Private information"*] means information[, including a formula, pattern, compilation, program, device, method, technique, or process,] that:

(i) [derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use] [*has personal value in limitation of its acquisition, disclosure or use and is not readily accessible by the public*], and

(ii) is the subject of efforts that are reasonable under the circumstances to maintain its [secrecy] [*privacy*].[5]

"Personal value" might be open-ended to "include emotional, economic or reputational value."

[3] UTSA Official Text § 1(2) (emphasis added).

[4] UTSA Official Text § 1(1) (emphasis added).

[5] UTSA Official Text § 1(4) (emphasis added). Unlike "trade secrets" as defined in the Economic Espionage Act, 18 U.S.C. § 1839(3) (listing of "types" of information), which the recent Defend Trade Secrets Act of 2016 created a federal private right of action for "misappropriation" defined almost identically to the UTSA (compare 18 U.S.C. § 1839(5), the UTSA trade secrets may be any information having economic value and subject to reasonable efforts to maintain secrecy. "Secrecy" is not defined except as bootstrapped from this definition of not being disclosed so as to be "generally known to" or "readily ascertainable by proper means by" the class of persons recited in clause (i). A contractual or relationship-based duty of confidentiality may suffice.

I proposed this template for use in addressing unreasonable drone surveillance in the Drone Regulation study, considering that unexpected aerial surveillance is one of the few recognized non-fraud, non-trespassory "improper means" of information acquisition under UTSA.[6]

I suggest that this template be considered for the Unauthorized Disclosure of Intimate Images (UDII) drafting project. Even if "private information" is limited to "intimate images," the template would cover both improper or fraudulent acquisition or creation of the information (photograph) as well as breach of confidence in unauthorized disclosure or use, and address third parties with notice even after if acquired innocently, as by mistake. Well-established UTSA (and earlier) considerations of value and expectations may be applied and be balanced against First Amendment considerations as well as Section 230 of the Communication Decency Act, because the focus us not on publication, but on "misappropriation" ("theft" and breach of confidence).

A narrower tailoring of the proposed template to "intimate image" might be the following, which I cross-reference to the March meeting draft:

"Misappropriation" means:

(i) acquisition of an intimate image of another by a person who knows or has reason to know that it was acquired or produced by improper means; [*This goes beyond UDII to address improper acquisition without actual use and extends to Photoshopped images.*] or

(ii) disclosure or use of the intimate image of another without express or implied consent by a person who

(A) used improper means to acquire the intimate image [*cf. UDII §3(a)(1)(C)*]; or

(B) at the time of disclosure or use, knew or had reason to know that his possession of the intimate image was

(I) derived from or through a person who had utilized improper means to acquire it;

(II) acquired under circumstances giving rise to a duty to maintain its privacy or limit its use; or

(III) derived from or through a person who owed a duty to the person seeking relief to maintain its privacy or limit its use [*These address UDII §3(a)(1)(D including third party use)*]; ; or

(C) before a material change of his position, knew or had reason to know that it was private and that knowledge of it had been acquired by accident or mistake. [*This reaches hosts with knowledge or notice where "material*

[6] E.I. du Pont de Nemours & Co. v. Christopher, 431 F.2d 1012, 1015-17 (5th Cir. 1970) (The Supreme Court of [Texas] has declared that "the undoubted tendency of the law has been to recognize and enforce higher standards of commercial morality in the business world."), cited in the UTSA Official Comments and by the Supreme Court at Kewanee Oil Co. v. Bicron Corp.. 416 U.S. 470, 475-76 (1976). While local expectations regarding aerial surveillance may or may not have changed, the underlying concept that acquisition of information by "improper means" is "misappropriation" applies in all the States now under both state and federal law.

change might be limited to some inability not to take down or redact; downstream hosters may be liable after notice.]

"Improper means" includes theft, bribery, misrepresentation, false pretenses, breach or inducement of a breach of a duty to maintain privacy, espionage through electronic or other means, or unauthorized access to or exceeding authorized use of the property, including stored or communicated information, of another.

"Intimate image" means a~~n~~ visual image, credibly real, in which a person is depicted in which the person's intimate parts are exposed or the person is engaged in sexual conduct and ~~the depicted person~~in or for which one or more persons is identifiable from the image itself or from information made available with the image. Consent for disclosure of such an image is required from each person identifiable in or from the image to be disclosed." [*cf. UDII §3(a)(1)(A) and –(B).*]

Threatened misappropriation is actionable under UTSA, but primarily for injunctive relief. Whether a threat itself should be actionable under UDII for damages when not actually consummated may be subject to debate. ~~Possibly multiple threats~~Generally, inchoate offenses are part of criminal law, as is extortion. Here, probably more than one threat by the ex-boyfriend might be required by legislators for civil liability.

An advantage to using the UTSA template is the current momentum behind it, particularly in the overwhelming support of Congress to add UTSA-type "misappropriation" to the Economic Espionage Act. Clearly the legislators and the ISPs wouldn't want their trade secrets (actually, confidential information of economic value) trafficked under the protection of CDA. The Brandeis/Prosser causes for invasion of privacy are largely specialized misappropriations. The intrusion aspect was added to trade secrets in the UTSA stand-alone cause of "acquisition by improper means."

We might wish to characterize the underlying wrong as "misappropriation" (improper means and breach of confidence) rather than "disclosure" that invokes the First Amendment and CDA.

The issue for extension of UTSA-type misappropriation is whether personal privacy values can and should be protected similarly to commercial privacy values. Reputation value is important, both personally and in the commercial context – it is the basis for injunction (irreparable injury) since the Supreme Court eliminated injunctions for simple infringement.

The UTSA provision for reasonable royalties in lieu of actual (lost profit or unjust enrichment) damages also may be applied (or the copyright concept of statutory damages).