Перуджански журналистически принципи

Работа с лица, подаващи сигнали за нередности (whistleblowers), в дигиталната ера

blueprint for FREE SPEECH

12 ПРИНЦИПА ЗА РАБОТА С ЛИЦА, ПОДАВАЩИ СИГНАЛИ ЗА НЕРЕДНОСТИ (WHISTLEBLOWERS), В ДИГИТАЛНАТА ЕРА

АВТОРИ

Д-р Джули Посетти
Старши научен сътрудник в Институт за изследване на журналистиката „Ройтерс“ към Оксфордския университет

Д-р Суелет Драйфус
Научен сътрудник, Университет в Мелбърн. Изпълнителен директор, Blueprint for Free Speech

Наоми Колвин
Програмен директор във Великобритания, Blueprint for Free Speech

1

Защитете източниците си. Защитавайте анонимността.

Ангажиментът на журналиста да защитава анонимността на поверителните източници и лицата, подаващи сигнали за нередности, трябва да бъде нарушен само при най-изключителни обстоятелства.

Съсредоточете се върху собствената си цифрова безопасност, за да избегнете неволното разобличаване на Вашия конфиденциален източник.

Съзнавайте, че дори да работите по най-високите стандарти за цифрова сигурност, може да не сте в състояние да защитите поверителния източник от идентифициране.

blueprint for FREE SPEECH

2 Осигурете безопасни начини за източниците Ви да осъществят „първи контакт“.

Първият контакт често е средството, чрез което журналист и подател на сигнали за нередности могат да бъдат свързани на по-късен етап от разследването, дори ако и двамата използват криптиране.

Помогнете на потенциалните лица, подаващи сигнали за нередности, като оповестите начини, по които могат да се свържат с Вас, като използват анонимни и криптирани канали.

Включете цифрови адреси, потребителски имена или публични ключове в своята обществено достъпна контактна информация.

Обявете предварително кога ще присъствате на публични събития лично.

Говорете за широкото влияние на заплахите за конфиденциалността в дигиталната ера, които подкопават правото на обществото да узнае информация поради компрометирана поверителност на източниците.

3

Разбирайте цената, която плащат подаващите сигнали за нередности, помогнете на източниците си да осъзнаят какво ще се случи, когато историята стане публична.

Отнасяйте се към лицето, което се излага на значителен риск, за да Ви повери своята информация в обществен интерес и да Ви разкрие своята идентичност, с достойнство и уважение.

Помислете за своята отговорност и за издателя си, за да осигурите сигурността и правната защита (където е уместно) на Вашите източници.

Във всички стадии на журналистическата работа обсъждайте развитието на историята и възможните правни рискове с редакторите си.

blueprint for FREE SPEECH

4 Фокусирайте се върху обществената стойност на информацията, а не върху отношението или мнението на Вашия източник.

Не отхвърляйте информация, предоставена от източник, защото не сте съгласни с неговите мотиви, философия, нагласа или публични изявления. Въпреки че информацията трябва да се преценява по същество, остава важно да се оцени мотивацията на Вашия източник.

Бъдете наясно с възможността за неточности в информацията и данните, включително в предоставянето на злонамерени такива.

Уверете се, че прилагате същите стандарти за проверка преди публикуването на информацията, предоставена от конфиденциален източник, както бихте направили за всяка информация или свидетелски показания.

Бъдете отговорни към цифровата си защита и използвайте криптиране.

5

Криптирането защитава свободата на словото, но не е гаранция за поверителност. Следите на цифрови данни могат да доведат до откриването на идентичността на източника. Използвайте криптиране в цифрови комуникации с поверителни източници и лица, подаващи сигнали за нередности, но имайте предвид неговите ограничения, особено когато става въпрос за метаданни.

Давайте добър пример и на други журналисти в това отношение. Избягвайте ненужни публикации за борба с тероризма или засягащи националната сигурност, които могат да се използват за оправдаване за премахването на криптирането и свързаните с тях нарушения на поверителността, които подкопават разследващата журналистика.

blueprint for FREE SPEECH

6

Определете най-големите заплахи за Вас и за Вашия източник. Вземете мерки, за да защитите и двамата.

Направете оценка на рисковете за историята, по която работите, и за източника, с който работите.

Обмислете кога да използвате аналагови комуникационни практики като срещи лице в лице.

Използвайте организации като The Signals Network, които се стремят да улеснят връзките между лицата, подаващи сигнали за нередности, журналистите, експертите по сигурността и специализираните адвокати.

7

Обяснете рисковете от използването на цифрови технологии на Вашия източник или подател на сигнали. Обучете своите подаващи сигнали контакти в основни принципи за дигитална сигурност.

Обяснете рисковете от използването на цифрови комуникации по отношение на потенциално прихващане, проследяване, целенасоченото наблюдение и използването на метаданни.

Уверете се, че Вашият източник е наясно с всички цифрови инструменти, които използвате за комуникация.

Обяснете какво могат и какво не тези инструменти.

Помогнете на източника си да разбере рисковете от цифровата комуникация, които се отнасят до конкретната ситуация, в която се намира той.

Обмислете споделянето на ресурси, очертаващи защитни техники, за да подкрепите самостоятелното обучение на Вашия източник.

.

blueprint for FREE SPEECH

8 Публикувайте оригинални документи и бази данни, когато това е възможно и безопасно.

Използвайте статистически методи за добра визуализация, които позволяват на читателите да разберат значението на целия набор от данни.

Бъдете отворени за международни сътрудничества по отношение на големи масиви от данни, които също биха могли да се възползват от тях.

Правете общодостъпни архиви на оригиналния материал с възможности за споделяне.

Бъдете наясно с рисковете, свързани с публикуването на оригинални масиви от данни и правете така, че да ги предотвратявате.

9

Внимателно и безопасно изтривайте данните, предоставени от източници, когато те са поискали това, в съответствие с етичните, правните и работодателските изисквания.

Документите и техните метаданни могат да се използват за идентифициране на техния източник. Бъдете внимателни как и къде ги споделяте.

Съветвайте се по технически въпроси. Шифровайте данните, съхранени на твърдия диск на компютъра или на преносими устройства.

Изтриването на данни във Вашата операционна система не означава, че не могат да бъдат възстановени.

Когато е необходимо, осигурете правилното изтриване на данните, за да се уверите, че не могат да бъдат възстановени.

При наличие на високорискова информация може да се наложи да унищожите устройството, за да гарантирате сигурното изтриване.

blueprint for FREE SPEECH

10 Уверете се, че дигиталните платформи за подаване на сигнали (drop boxes) предлагат добро ниво на сигурност и анонимност.

Съществуват редица налични платформи, които позволяват на източниците да изпращат документи на журналистите и да продължават да общуват с тях, без да разкриват своята самоличност.
Повечето използват мрежата Tor или друга подобна система.

Посъветвайте се по техническите въпроси преди да инсталирате подобна платформа и разберете какво е необходимо, за работата с нея.

Осигурете ясни инструкции за източниците си за това как да използват безопасно платформата, както и какви са потенциалните рискове.

Това може да включва публикуване на обяснителни бележки или видеоклипове на уебсайта Ви.

11

Запознайте се с правните и регулаторни рамки за защита на поверителни източници и лица, подаващи сигнали за нередности..

Запознайте се със законите за защита на източниците и лицата, подаващи сигнали за нередности, във Вашия регион и в международен план.

Разберете кои права на ниво ООН, които се прилагат офлайн, също се прилагат и онлайн.

Направете така, че Вашият източник да знае за правната защита, която може да получи, ако съществува такава.

Информирайте за мерките, които трябва да се вземат на законодателно ниво за осигуряване на по-добра защита на лицата, подаващи сигнали за нередности.

blueprint for FREE SPEECH

12 Насърчавайте издателите да осигурят подходяща сигурност на данните и необходимото обучение за журналистите.

Настоявайте за приемането на редакционни правила и принципи, които да признават заплахите, които съществуват при защитаването на източниците в дигиталната ера.

Разкажете за правните и редакционни заплахи при наличие на бездействие по тези въпроси.

Ако сте редактор или издател, реагирайте по подходящ начин при разглеждането на рисковете.

Уверете се, че Вашата организация има стратегия за защита на дигиталната сигурност, която интегрира аналоговата сигурност, цифровата сигурност, правната политика и обучението на служителите.

Ако сте журналист на свободна практика, свържете се със своя синдикат или с неправителствена организация за помощ.

БЛАГОДАРНОСТИ

Инициатива „Отворено общество за Европа“ в рамките на Фондация „Отворено общество“, Институт за изследване на журналистиката „Ройтерс“ към университета в Оксфорд, Фондация „Томсън Ройтерс“, Университетът в Мелбърн, Nishith Desai Associates и S. Welsh.

ПАРТНЬОРСКИ ОРГАНИЗАЦИИ

Институт за изследване на журналистиката „Ройтерс“ (RISJ) към Оксфордския университет, Международния център за журналисти (ICFJ), Глобална мрежа за разследваща журналистика (GIJN), Световния форум за редактори, The Signals Network

ИЗТОЧНИЦИ

BlueprintForFreeSpeech.net
TheSignalsNetwork.org
UNESCO's Protecting Journalism Sources in the Digital Age (2017)
https://en.unesco.org/unesco-series-on-internet-freedom

blueprint for FREE SPEECH

Произход на Перуджански журналистически принципи

Перуджански журналистически принципи са разработени от авторите в партньорство с екип от 20 международни журналисти и експерти, организиран от Blueprint for Free Speech, в рамките на Международния журналистически фестивал в Перуджа, Италия, преведен през април 2018 г. В последствие авторите провеждат допълнителни консултации с широк кръг разследващи журналисти, юридически и академични общности, за да усъвършенстват принципите.

blueprint for FREE SPEECH