Перуджийские принципы для журналистов:

Работа с разоблачителями в эпоху цифровых технологий

blueprint for FREE SPEECH

12 ПРИНЦИПОВ ДЛЯ РАБОТЫ С РАЗОБЛАЧИТЕЛЯМИ В ЭПОХУ ЦИФРОВЫХ ТЕХНОЛОГИЙ

Авторы

Джули Посетти
Старший научный сотрудник Института изучения журналистики Reuters в Оксфордском университете

Доктор Суэлетт Дрейфус
Научный сотрудник, Университет Мельбурна. Исполнительный директор, Blueprint for Free Speech

Наоми Колвин
Программный директор в Великобритании, Blueprint for Free Speech

1

Защита своих источников. Защита анонимности.

Обязанность журналиста защищать анонимность конфиденциальных источников и разоблачителей должна нарушаться только в самых крайних обстоятельствах.

Сосредоточьтесь на собственной цифровой безопасности, чтобы избежать случайного разглашения вашего конфиденциального источника.

Помните, что даже если вы действуете в соответствии с самыми высокими стандартами цифровой безопасности, вы не сможете защитить конфиденциального источника от идентификации.

blueprint for FREE SPEECH

2 Предоставьте источникам более безопасный способ «первого контакта».

Первый контакт часто является способом, с помощью которого журналист и разоблачитель могут быть связаны в дальнейшем расследовании, даже если они оба использовали шифрование.

Помогите потенциальным разоблачителям, сообщив им, как они могут связаться с вами по анонимным и зашифрованным каналам. Включите цифровые адреса, имена пользователей или открытые ключи в свои общедоступные контактные данные.

Заранее сообщайте, когда будете лично присутствовать на публичных мероприятиях.

Сообщайте о широком влиянии угроз конфиденциальности в цифровую эпоху подрывающих право общественности на информацию путем компрометации источника.

3

Понимайте цену разоблачения, помогайте источникам информации продумать, что произойдет, когда история станет достоянием гласности.

С достоинством и уважением относитесь к человеку, который подвергается значительному риску, чтобы доверить вам свои секреты и личные данные с целью раскрытия информации в интересах общества.

Проанализируйте свою ответственность и обязательства издателя по защите источников и защите ваших прав (в соответствующих обстоятельствах).

На всех стадиях журналистской работы обсуждайте с редакторами свой материал и возможные юридические риски.

blueprint for FREE SPEECH

4 Сконцентрируйтесь в первую очередь на общественной значимости информации, а не на позиции или мнении вашего источника.

Не сбрасывайте со счетов информацию, предоставленную источником, по той причине, что вы не согласны с ее мотивом, убеждениями, взглядами или публичными заявлениями.

Информацию следует оценивать по существу, но при этом важно также учитывать и мотивацию вашего источника. Помните о вероятных неточностях в базах данных, в том числе и зараженных.

Убедитесь, что вы используете те же методы предварительной проверки информации, что и в отношении других данных или сведений, предоставляемых анонимным источником, что и в отношении любого другого свидетеля.

5

Возьмите на себя ответственность за свою компьютерную безопасность и используйте шифрование

Шифрование защищает свободу прессы, но не является гарантией конфиденциальности. Цифровые данные могут быть использованы для того чтобы раскрыть личность источника.

Используйте шифрование в электронной коммуникации с анонимными источниками и разоблачителями, но помните о существующих недостатках, особенно когда речь идет о метаданных.

В качестве примера для других журналистов в этом отношении приводится успешная практика.

Избегайте ненужных статей о борьбе с терроризмом или национальной безопасности, которые используются для оправдания использования шифрования и связанных с ним попыток вмешательства в частную жизнь, которые подрывают журналистские расследования.

blueprint for FREE SPEECH

6

Определите самые большие угрозы вам и вашему источнику. Примите меры, чтобы защитить вас обоих.

Проведите оценку риска для материала, над которым вы работаете, и для источника, с которым вы работаете.

Подумайте, когда следует использовать традиционные методы коммуникации, такие как встреча лицом к лицу.

Используйте такие сети, как The Signals Network, которые помогают упростить связь между разоблачителями, журналистами, экспертами по безопасности и специализированными юристами.

7

Рассказывайте о рисках, связанных с использованием цифровых технологий для связи с источником или разоблачителем. Обучайте разоблачителей основным правилам цифровой безопасности.

Объясните риски электронной коммуникации с точки зрения возможности ее перехвата, наблюдения, адресного контроля и передачи метаданных.

Убедитесь, что ваш источник уверен в надежности цифровых средств связи, которые вы используете для общения.

Объясните, на что способны эти инструменты, а на что - нет. Помогите своему источнику понять риски, связанные с цифровой коммуникацией, которые могут возникнуть в его конкретной ситуации.

Рассмотрите о возможности совместного использования ресурсов, в которых описываются методы защиты, чтобы поддержать самостоятельную подготовку источника.

blueprint for FREE SPEECH

8. Публикуйте оригиналы документов и баз данных там, где это целесообразно и безопасно.

Использовать статистические методы и методы визуализации данных, которые позволяют читателям понять значение всего объёма информации.

Будьте открытыми для международного сотрудничества, связанного с большими объемами данных, которые могут быть полезны с других точек зрения.

Сделайте общедоступными архивы исходных материалов с возможностью поиска.

Помните о рисках, связанных с публикацией оригинальных баз данных, и работайте над тем, чтобы их уменьшить.

9

Надежное и безопасное удаление данных, предоставленных источником по запросу, в соответствии с этическими, правовыми обязательствами и требованиями работодателя.

Документы и их метаданные могут быть использованы для идентификации источника. Будьте осторожны, как и где вы делитесь ими. Обратитесь за техническим советом. Всегда шифруйте данные, хранящиеся на жестком диске компьютера или портативном устройстве, таком как USB или телефон. Включите полное шифрование диска.

Удаление данных в операционной системе могут быть восстановлены. Обратитесь за помощью к экспертам, чтобы убедиться, что данные надежно стерты и не могут быть восстановлены.

Для получения информации с высоким уровнем риска может потребоваться уничтожить запоминающее устройство, чтобы обеспечить его удаление. Для получения информации высокого риска вам может потребоваться уничтожить устройство хранения, чтобы обеспечить его удаление.

blueprint for FREE SPEECH

10 Убедитесь, что цифровые дропбоксы обеспечивают высокий уровень безопасности и анонимности.

Существует ряд систем “дропбоксов”, которые позволяют источникам отправлять документы журналистам и продолжать общаться с ними, не раскрывая их личности. Большинство используют сеть Tor или другую подобную систему.

Получите техническую консультацию перед установкой дропбокса и узнайте, что требуется для его правильного функционирования.

Предоставьте четкие инструкции для источников о том, как безопасно использовать ваш дропбокс и также расскажите о его потенциальных рисках. Это может включать предоставление разъяснительных комментариев или видеоматериалов на вашем веб-сайте.

11

Ознакомьтесь с нормативно-правовой базой для защиты конфиденциальных источников и разоблачителей.

Ознакомьтесь с законодательством о защите источников информации и законами о защите разоблачителей в вашем регионе и за рубежом. Узнайте, какие права, применяемые на уровне ООН в оффлайновом режиме, действуют и в онлайн-режиме.

Сообщите вашему источнику об открытых для него возможностях правовой защиты, если таковые существуют.

Сообщите о мерах по улучшению защиты разоблачителей в правовом поле.

blueprint for FREE SPEECH

12 Стимулировать редакторов СМИ к предоставлению журналистам надлежащей защиты своих данных и соответствующего обучения.

Настаивайте на принятии редакционных правил и принципов, которые признают существование угроз для защиты источников в цифровую эпоху.

Расскажите о юридических и редакционных угрозах в связи с бездействием в этих вопросах.

Если вы редактор или издатель, реагируйте на риски соответствующим образом.

Убедитесь, что в вашей организации есть

стратегия защиты безопасности в сфере цифровых технологий, которая включает в себя аналоговую защиту, цифровую безопасность, правовую политику и подготовку кадров.

Если вы внештатный журналист, обратитесь за помощью в профсоюз или неправительственную общественную организацию.

Благодарности

Инициатива “Открытое общество для Европы” в рамках Фондов открытого общества, Институт Рейтерс по изучению журналистики при Оксфордском университете,

Фонд Томсона Рейтерса, Университет Мельбурна,

Нишит Десаи Ассошиэйтс и С. Уэльс.

Партнерские организации Фонда

Институт Рейтер по изучению журналистики (RISJ) при Оксфордском университете, Международный центр журналистов (ICFJ), Глобальная сеть журналистов-расследователей (GIJN), Всемирный форум редакторов, The Signals Network.

Ресурсы

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

Источник происхождения Перуджийских принципов

Перуджийские принципы были разработаны авторами в партнерстве с Круглым столом 20 международных журналистов и экспертов, организованным Blueprint for Free Speech в рамках Международного фестиваля журналистики в Перудже, Италия, в апреле 2018 года.

Затем авторы провели консультации с более широким кругом журналистов, занимающихся расследованиями, юристов и ученых с целью уточнения Принципов.

blueprint for FREE SPEECH