Los principios de Perugia para el Periodismo:

trabajando con alertadores en la era digital

blueprint for FREE SPEECH

12 PRINCIPIOS PARA TRABAJAR CON ALERTADORES EN LA ERA DIGITAL.

Autores

Julie Posetti

Investigador Principal, Reuters Institute for the Study of Journalism de la Universidad de Oxford

Dra. Suelette Dreyfus

Especialista Académico, Universidad de Melbourne. Directora Ejecutiva, Blueprint for Free Speech

Naomi Colvin

Directora del Programa del Reino Unido, Blueprint for Free Speech

1

Proteja sus fuentes. Defienda el anonimato.

Concéntrese en su propia seguridad digital para evitar causar inadvertidamente el desenmascaramiento de su fuente confidencial.

Reconozca que incluso si usted opera con los más altos estándares de tecnología digital, tal vez no pueda proteger una fuente confidencial de ser identificada.

El compromiso de un periodista de proteger el anonimato de las fuentes confidenciales y de los alertadores sólo debe ser violado en las circunstancias más excepcionales.

blueprint for FREE SPEECH

2 Proporcione formas más seguras para las fuentes a la hora de hacer "primer contacto".

El primer contacto es frecuentemente el medio por el cual un periodista y un informante pueden ser vinculados en una investigación posterior, incluso si ambos usan encriptación.

Ayude a los alertadores potenciales publicando las formas en que pueden ponerse en contacto con usted a través de canales anónimos y encriptados. Incluya direcciones digitales, nombres de usuario o claves públicas en sus datos de contacto públicos.

Anuncie con anticipación cuándo estará en eventos públicos en persona.

Informe sobre las amplias implicaciones de las amenazas a la privacidad en la Era Digital que socavan el derecho del público a saber, comprometiendo la confidencialidad de la fuente.

3

Reconozca los costes de alertar, ayude a las fuentes a pensar en lo que sucede cuando se publica la historia.

Tratar a la persona que asume un riesgo significativo para confiarle sus secretos y su identidad en un esfuerzo por revelar información de interés público con dignidad y respeto.

Considere sus responsabilidades, y las de su editor, para asegurar la seguridad de sus fuentes y la defensa legal (cuando sea relevante).

Discuta la historia y los posibles riesgos legales con sus editores al principio del proceso de presentación de reportes.

blueprint for FREE SPEECH

4 Enfóquese en el interés público de la información, en lugar de las actitudes u opiniones de su fuente.

No descarte la información suministrada por una fuente porque no esté de acuerdo con sus motivos, filosofías, actitudes o declaraciones públicas.

Si bien la información debe juzgarse por sus méritos, sigue siendo importante evaluar la motivación de su fuente. Tenga en cuenta la posibilidad de inexactitudes en los conjuntos de datos, incluidos los maliciosos.

Asegúrese de aplicar a la información proporcionada por una fuente confidencial los mismos estándares de verificación previa que a cualquier cuenta de datos o testigos.

Asuma la responsabilidad de su defensa digital y use encriptación.

5

La encriptación defiende la libertad de prensa, pero no es una garantía de confidencialidad. Los rastros de datos digitales pueden llevar a descubrimiento de la identidad de una fuente.

Use encriptación en los sistemas digitales de comunicaciones con fuentes confidenciales y alertadores, pero tenga en cuenta sus limitaciones, especialmente en lo que respecta a los metadatos.

Modelar buenas prácticas para otros periodistas en este respecto.

Evite reportar sin criterio sobre las narrativas antiterroristas o de seguridad nacional utilizadas para justificar las invalidaciones del cifrado y las violaciones de la privacidad asociadas, que socavan la capacidad de investigación periodística.

blueprint for FREE SPEECH

6

Determine las mayores amenazas para usted y su fuente. Tome medidas para proteger a ambos.

Realice una evaluación de riesgos para la historia en la que está trabajando y la fuente con la que está trabajando.

Considere cuándo utilizar las prácticas de comunicación de la era analógica, como las reuniones cara a cara.

Hacer uso de organizaciones como The Signals Network, que buscan facilitar las relaciones entre alertadores, periodistas, expertos en seguridad, y abogados especialistas.

7

Explique los riesgos de exposición digital a su fuente o alertador. Entrene a sus alertadores en seguridad digital básica.

Explique los riesgos de la comunicación digital en términos de interceptación, vigilancia masiva, vigilancia de objetivos y entrega de metadatos.

Asegúrese de que su fuente tenga confianza en cualquier herramienta digital que esté utilizando para comunicarse. Explique lo que esas herramientas pueden hacer y lo que no. Ayude a su fuente a comprender los riesgos de la comunicación digital que se aplican a su situación particular.

Considere la posibilidad de compartir recursos para esbozar técnicas defensivas que apoyen las actividades de aprendizaje autodidacta de su fuente.

blueprint for FREE SPEECH

8

Publique documentos originales y conjuntos de datos cuando sea posible y seguro hacerlo.

Utilice técnicas estadísticas y de visualización de datos que permitan a los lectores comprender la importancia de todo un conjunto de datos.

Esté abierto a colaboraciones internacionales y de otro tipo en torno a grandes conjuntos de datos, que pueden beneficiarse de una amplia gama de perspectivas.

Poner a disposición del público archivos de material original que permitan realizar búsquedas.

Sea consciente de los riesgos que conlleva la publicación de conjuntos de datos originales y trabaje para mitigarlos.

9

Borre de forma segura los datos proporcionados por las fuentes, cuando se le pida, de acuerdo con las obligaciones éticas, legales y del empleador.

Los documentos y sus metadatos pueden utilizarse para identificar su origen. Tenga cuidado de cómo y dónde los comparte. Obtenga asesoramiento técnico.

Siempre cifre los datos almacenados en el disco duro de su ordenador o en un dispositivo portátil. Active la encriptación completa de su disco.

La eliminación de datos dentro de su sistema operativo significa que aún pueden recuperarse. La eliminación segura sobrescribe los datos varias veces para asegurarse de que no se puedan recuperar. Si es necesario, elimine los datos de forma segura para asegurarse de que no se puedan recuperar.

En cuanto a la información de alto riesgo, es posible que deba destruir el dispositivo de almacenamiento para garantizar su eliminación.

blueprint for FREE SPEECH

10

Asegúrese de que los buzones digitales ofrezcan un buen nivel de seguridad y anonimato.

Hay varios sistemas de buzones disponibles que permiten a las fuentes enviar documentos a los periodistas y seguir comunicándose con ellos sin revelar su identidad. La mayoría hace uso de la red Tor, u otro sistema similar.

Obtenga asesoramiento técnico antes de instalar un buzón y entienda lo que es necesario para su funcionamiento, y mantenimiento.

Proporcione instrucciones claras a las fuentes sobre cómo usar su buzón de manera segura y los riesgos potenciales. Esto podría incluir la publicación de notas explicativas o vídeos en su sitio web.

11

Entienda las normas legales y marcos regulatorios para la protección de fuentes confidenciales y denunciantes.

Familiarícese con las leyes de protección de las fuentes y de alerta de irregularidades en su región y a nivel internacional, entendiendo que las declaraciones de la ONU se aplican tanto en entornos digitales como analógicos.

Hágale saber a su fuente acerca de las leyes protecciones disponibles para ellos, si es que existen.

Informe sobre los esfuerzos para asegurar una mejor protección de los alertadores en la ley.

blueprint for FREE SPEECH

12

Alentar a los editores para que proporcionen seguridad de los datos y una formación adecuada para los periodistas.

Insistir en la adopción de políticas y guías en las salas de redacción, que reconozcan las amenazas de la era digital para la protección de las fuentes.

Destacar las amenazas legales y editoriales del exceso de confianza en estos temas.

Si usted es editor, responda adecuadamente a los riesgos.

Asegúrese de que su organización tiene una estrategia de defensa de la seguridad digital que integra la seguridad analógica, la seguridad digital, las leyes jurídicas y la formación.

Si usted es un periodista independiente, póngase en contacto con su sindicato o con una ONG para obtener ayuda.

Agradecimientos

The Open Society Initiative for Europe within the Open Society Foundations, The Reuters Institute for the Study of Journalism at the University of Oxford, The Thomson Reuters Foundation, The University of Melbourne, Nishith Desai Associates and S. Welsh.

Organizaciones socias fundadoras

Reuters Institute for the Study of Journalism (RISJ) de la Universidad de Oxford, International Center for Journalists (ICFJ), Global Investigative Journalism Network (GIJN), World Editors Forum, The Signals Network

Recursos

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

El origen de los Principios de Perugia

Los Principios de Perugia fueron desarrollados por los autores en colaboración con una mesa redonda de 20 periodistas y expertos internacionales organizada por Blueprint for Free Speech durante el Festival Internacional de Periodismo en Perugia, Italia, en abril de 2018.

Los autores luego consultaron con las comunidades más amplias del periodismo de investigación, el derecho y el mundo académico para perfeccionar los Principios.

blueprint for FREE SPEECH