"The Case for Cybersecurity Policies"[1]
Description of Database

Asaf Lubin[2] and Meirav Furth-Matzkin[3]

In *The Case for Cybersecurity Policies* we ask how Internet of Things (IoT) vendors disclose information about their cybersecurity practices to their consumers and the general public. We would expect in a competitive market that vendors would provide the necessary security protections as a function of consumer demand (and the associated willingness to pay more for such security features). At the same time, consumers are often unaware of their potential cybersecurity and information privacy risks and the degree to which they are vulnerable to potential harms. This is especially true for IoT devices, which by their very design involve a complex multilayered hardware and software and an inability to control security along the product's supply chain and life cycle. We therefore sought to explore whether IoT vendors are transparent as to their cybersecurity policies so to increase both regulatory and public understanding of potential vulnerabilities associated with these products and of the companies' safety measures.

To support this research we have created an original database of the legal documents of a diverse representation of IoT companies. We began by purchasing a commercial database of 349 publicly traded companies (on one or more stock exchange) prepared by "IoT Analytics", a German-based provider of market insights and strategic business intelligence for the IoT industry. This database was selected because of its broad geographical scope: 47% of the companies in the database are in North America, 27% in Europe, 25% in Asia, and 1% in the Rest of the World.[4] The dataset also provides diversity in segment focus, with the IoT companies covering an array of key industries including smart home (16%), mobility and connected vehicles (11%), lifestyle and wearable tech (8%), smart city (6%), connected health (6%) and industrial solutions. (6%). In so doing, the database is, to our knowledge, the most robust and diverse commercial set currently available for purchase.[5]

Moreover, lacking a uniform definition of "IoT company" the producers of this dataset adopted an expansive interpretation of the term that encompasses the entirety of the supply chain. The database creators' included companies that are either "selling Internet of Things enabled products, play a vital part in the IoT technology infrastructure, or act as an enabler to the Internet of Things development."[6] The final database includes 150 companies that market their own IoT-

[1] This work was supported by The Federmann Cyber Security Center in conjunction with the Israel National Cyber Directorate.

[2] Dr. Asaf Lubin is an Associate Professor of Law at Indiana University Maurer School of Law, an Affiliated Fellow at the Information Society Project, Yale Law School, a Faculty Associate at the Berkman Klein Center for Internet and Society at Harvard University, and a Visiting Scholar at Hebrew University Feuermann Cybersecurity Research Center.

[3] Dr. Meirav Furth-Matzkin is an Assistant Professor of Law at the University of California Los Angeles Law School.

[4] Database Description, "Internet of Things Public Companies Database 2015", IOT ANALYTICS (Mar. 2015), available at: https://iot-analytics.com/product/database-iot-public-companies/.

[5] *Id.*

[6] *Id.*

enabled devices (43%), roughly 110 companies that manufacture hardware components (semiconductors, sensors, or communication hardware) (32%), and roughly 90 companies provide software (analytics, storage, IoT platforms) (25%).

The purchased database already included the following dimensions:

1. General information (company name, description, type and location).
2. Technology focus (Semiconductors, Sensors, Operating Systems, Analytics, Platform, Database, etc.).
3. Segment focus (Home, Lifestyle, Health, Mobility, Retail, Energy, Smart City, Industrial, etc.).
4. Enablement focus (Funding, Technology research, market research, distribution, consulting, incubation, etc.).
5. Further information (Founding date – only partially available, total funding – only partially available, ticker symbol, further comments, etc.).

The database has certain limitations. Most importantly, it was produced in 2015 and a few of the companies listed therein have either been acquired or merged or have shut down operations, making the information in the database obsolete. In addition, after reviewing the database, we were unable to determine in what fashion a few of the companies listed in the database were involved in the IoT market. In those scenarios we chose to remove the companies from the ultimate list. As a result the final dataset we have includes 315 companies.

For each of the companies on the database we downloaded all of the companies publicly available legal documentation including the companies' various terms of service, policies, and user agreements as available on their company websites (usually under the "legal" section). These legal documents were then coded, relying on the help of two research assistants. We attach as an annex the coding guidance we developed and relied upon throughout our coding. This guidance offers a detailed account of each of the columns in the database and what they represent.

As this is still a work-in-progress we are happy to discuss any issues or concerns relating to the database or our hypotheses. We may be reached at:

Dr. Asaf Lubin: lubina@iu.edu.

Dr. Meirav Furth-Matzkin: furth@law.ucla.edu.

Coding Guidance

Column	Instructions
D: Market Type	Entry: Best guess; use Crunchbase as a reference. *Try to use market types already identified for other, similar companies if possible.
BD: Does the company have a privacy policy?	Entry: “Yes” or “No”
BE: Is the privacy policy for the company, product, or website? If product, name the product(s).	Entry: “Company,” “Product: [Product Name],” “Website,” or “N/A” (if no PP) *If more than one PP is available, use the one for the company or product, not the website.
BF: Does the company have a Terms of Service or similar document?	Entry: “Yes” or “No”
BG: Are the Terms for the company, product, or website? If product, name the product(s) covered.	Entry: “Company,” “Product: [Product Name],” “Website,” or “N/A” (if no Terms) *If more than one Terms and Conditions is available, use the one for the company or product, not the website.
BH: Does the company have other cybersecurity- or data protection-related policy document(s)?	Entry: “Yes” or “No” *Examples of these kinds of documents are a separate cybersecurity policy, a vulnerability disclosure policy, etc. To locate, Google “site:[domain name] + cybersecurity/vulnerability policy.”
BI: Are other policy document(s), if any, for the company, product, or website? Enter N/A if answer to column BH is "No."	Entry: “Company,” “Product: [Product Name],” “Website,” “N/A” (if no other legal documents)
BJ: Were documents(s) found and downloaded to the database?	Entry: “Yes” or “No” *Naming conventions: “PP” for Privacy Policy, “ToS” for Terms of Service, “ToU” for Terms of Use, “T&C” for Terms and Conditions, and everything else written out; dates are formatted “DD” (downloaded date” or “ED” (effective date” followed by the date in MM.DD.YY format
BK: Does the company have a security or data protection clause?	Entry: “0,” “1,” “2,” or “3”

0 = No, 1 = Yes, on website but NOT in any policy documents, 2 = Yes, in website usage policy documents, 3 = Yes, in company-wide or product policy documents	*If the company has security or data protection clauses in both company/product and website usage policy documents, code as “3” and use the clauses in the company/product policy documents. (Company-wide or product-based policies take precedence over website usage policies.)
BL: In which documents, specifically, is the clause located? 0 = No clause, 1 = In PP, 2 = In Terms, 3 = In standalone policy, 4 = In PP & Terms, 5 = In PP & standalone policy, 6 = In Terms & standalone policy, 7= In PP, Terms, & standalone policy	Entry: “0,” “1”, “2”, “3”, “4”, “5,” “6,” “7”
BM: Security clause	Entry: “From [PP/Terms/etc.]: [security clause]” *Copy and paste each of the security clause(s), based on the answer to the previous column.
BN: Does the company identify as ISO 27001/2 compliant? 0 = No, 1 = Yes, on website but NOT in any policy documents, 2 = Yes, in website usage policy documents, 3 = Yes, in company-wide or product policy documents	Entry: “0,” “1,” “2,” or “3” *If the company has information about this security feature in several places (e.g., in both company/product and website usage policy documents), code as the highest possible value. (Again, company-wide or product-based policies take precedence over website usage information, which takes precedence over information that merely appears on a company webpage.)
BO: Does the company explicitly identify any of the ISO 27001:2013 security controls? 0 = No, 1 = Yes, on website but NOT in any policy documents, 2 = Yes, in website usage policy documents, 3 = Yes, in company-wide or product policy documents	Entry: “0,” “1,” “2,” “3” *If the company has information about this security feature in several places (e.g., in both company/product and website usage policy documents), code as the highest possible value. (Again, company-wide or product-based policies take precedence over website usage information, which takes precedence over information that merely appears on a company webpage.)
BP: If the company explicitly identifies ISO 27001:2013 security controls, which ones? Enter N/A if the answer to the previous column is no ("0").	Entry: “[list of controls]” or “N/A” *List is available in the database
BQ: Does the company identify as CIS20 compliant? (aka CSC, CCS CSC, SANS Top 20 or CAG 20) 0 = No, 1 = Yes, on website but NOT in any policy documents, 2 = Yes, in website usage policy documents, 3 = Yes, in company-wide or product policy documents	Entry: “0,” “1,” “2,” “3” *If the company has information about this security feature in several places (e.g., in both company/product and website usage policy documents), code as the highest possible value. (Again, company-wide or product-based policies take precedence over website usage information, which takes precedence over information that merely appears on a company webpage.)

BR: Does the company explicitly identify any of the CIS 20 security controls? 0 = No, 1 = Yes, on website but NOT in any policy documents, 2 = Yes, in website usage policy documents, 3 = Yes, in company-wide or product policy documents	Entry: “0,” “1,” “2,” “3” *If the company has information about this security feature in several places (e.g., in both company/product and website usage policy documents), code as the highest possible value. (Again, company-wide or product-based policies take precedence over website usage information, which takes precedence over information that merely appears on a company webpage.)
BS: If the company does explicitly identify CIS 20 security controls, which ones? Enter N/A if the answer to the previous column is no (“0").	Entry: “[list of controls]” or “N/A” *List is available in the database
BT: Does the company identify as compliant with any other cybersecurity standards or data protection standards? 0 = No, 1 = Yes, on website but NOT in any policy documents, 2 = Yes, in website usage policy documents, 3 = Yes, in company-wide or product policy documents	Entry: “0,” “1,” “2,” “3” *If the company has information about this security feature in several places (e.g., in both company/product and website usage policy documents), code as the highest possible value. (Again, company-wide or product-based policies take precedence over website usage information, which takes precedence over information that merely appears on a company webpage.)
BU: If the company does identify as compliant with other standards, which ones? Enter N/A if the answer to the previous column is no (“0").	Entry: “[list of standards],” “No specifics” (if no standards are explicitly named), or “N/A”
BV: Reference to encryption? 0 = No, 1 = Yes, on website but NOT in any policy documents, 2 = Yes, in website usage policy documents, 3 = Yes, in company-wide or product policy documents	Entry: “0,” “1,” “2,” “3” *If the company has information about this security feature in several places (e.g., in both company/product and website usage policy documents), code as the highest possible value. (Again, company-wide or product-based policies take precedence over website usage information, which takes precedence over information that merely appears on a company webpage.)
BW: If encryption is mentioned, is there reference to a cryptographic protocol (TLS/SSL) and its use in rest vs. in transit communications? Enter N/A if the answer to the previous column is "0" (no).	Entry: “[Encryption standard: at rest/in transit,” “No specifics” (if no standards are explicitly named), or “N/A”
BX: Reference to two-factor authentication? 0 = No, 1 = Yes, on website but NOT in any policy documents, 2 = Yes, in website usage policy documents, 3 = Yes, in company-wide or product policy documents	Entry: “0,” “1,” “2,” “3” *If the company has information about this security feature in several places (e.g., in both company/product and website usage policy documents), code as the highest possible value. (Again, company-wide or product-based policies take precedence over website usage information, which takes

	precedence over information that merely appears on a company webpage.)
BY: Reference to regular penetration testing by a third-party? 0 = No, 1 = Yes, on website but NOT in any policy documents, 2 = Yes, in website usage policy documents, 3 = Yes, in company-wide or product policy documents	Entry: "0," "1," "2," "3" *If the company has information about this security feature in several places (e.g., in both company/product and website usage policy documents), code as the highest possible value. (Again, company-wide or product-based policies take precedence over website usage information, which takes precedence over information that merely appears on a company webpage.)
BZ: Reference to mandatory change of passwords and other password-related good cyber hygiene practices? 0 = No, 1 = Yes, on website but NOT in any policy documents, 2 = Yes, in website usage policy documents, 3 = Yes, in company-wide or product policy documents	Entry: "0," "1," "2," "3" *If the company has information about this security feature in several places (e.g., in both company/product and website usage policy documents), code as the highest possible value. (Again, company-wide or product-based policies take precedence over website usage information, which takes precedence over information that merely appears on a company webpage.)
CA: Reference to a bug bounty program? 0 = No, 1 = Yes, on website but NOT in any policy documents, 2 = Yes, in website usage policy documents, 3 = Yes, in company-wide or product policy documents	Entry: "0," "1," "2," "3" *If the company has information about this security feature in several places (e.g., in both company/product and website usage policy documents), code as the highest possible value. (Again, company-wide or product-based policies take precedence over website usage information, which takes precedence over information that merely appears on a company webpage.)
CB: Is there a waiver of liability for third-party data collection/hacking/ vulnerabilities? 0 = No, 1 = Yes, on website but NOT in any policy documents, 2 = Yes, in website usage policy documents, 3 = Yes, in company-wide or product policy documents	Entry: "0," "1," "2," "3" *If the company has a waiver in several places (e.g., in both company/product and website usage policy documents), code as the highest possible value. (Again, company-wide or product-based policies take precedence over website usage information, which takes precedence over information that merely appears on a company webpage.)
CC: Waiver clause	Entry: "From [Terms/etc.]: [waiver clause]" or "N/A" (if the entry for the previous column is "0," no waiver of liability)
CD: Does this company offer a cybersecurity product/service?	Entry: "Yes" or "No"
CE: Has the company suffered a cyber attack or data breach that is publicly known?	Entry: "Yes" or "No"

CF: If the company has experienced a cyber breach, enter the article link here. Otherwise, enter N/A.	Entry: “http…” or “N/A”
CG: Comments	Entry: [Miscellaneous information]